Seamless Transition: Mastering Migration to Cisco Secure Firewall

Raghunath Kulkarni
Principal Engineer – Security TAC

Foster Lipkey
Principal Engineer – Security TAC

Session ID: BRKSEC-2058

Cisco Webex App

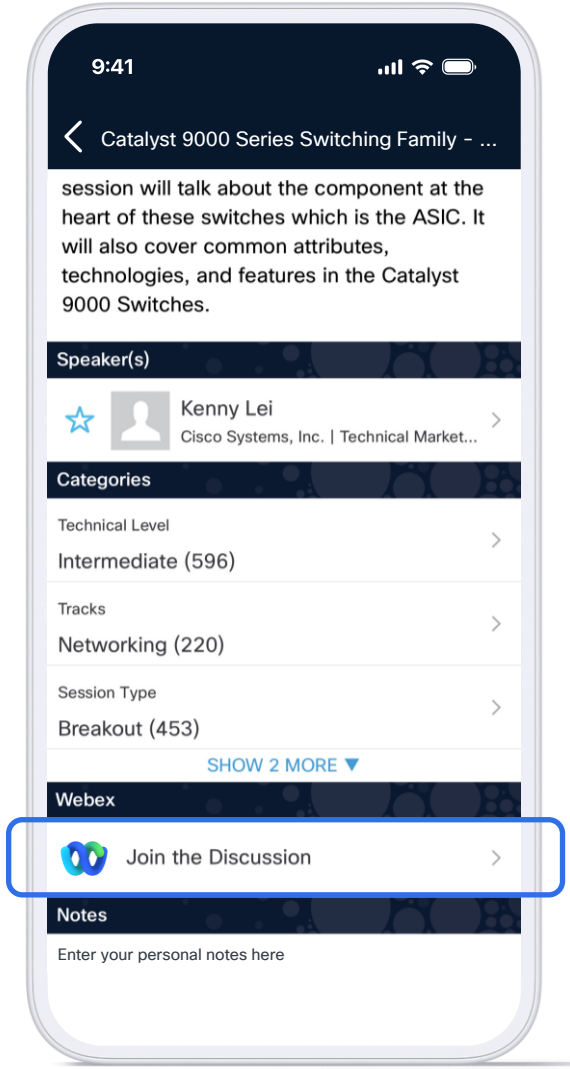
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKSEC-2058**

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Migration Lifecycle

02 Getting Started

03 Firepower Migration Tool

04 Firepower Device Migration

05 Bonus Content: Firepower Management Center Model Migration

06 References

© 2025 Cisco and/or its affiliates. All rights reserved.

Your Speaker(s)

Raghunath Kulkarni

Principal Engineer – Security TAC

- 15+ Years of Security Experience
- PIX -> ASA -> FWSM/ASA-SM -> Sourcefire ->FTD
- Sourcefire Veteran
- 2 Defensive Publications (UEBA & IoT Trust)
- 2 Cisco Patents (AI Identity & SecOps)
- Cisco Press Author in making

Foster Lipkey

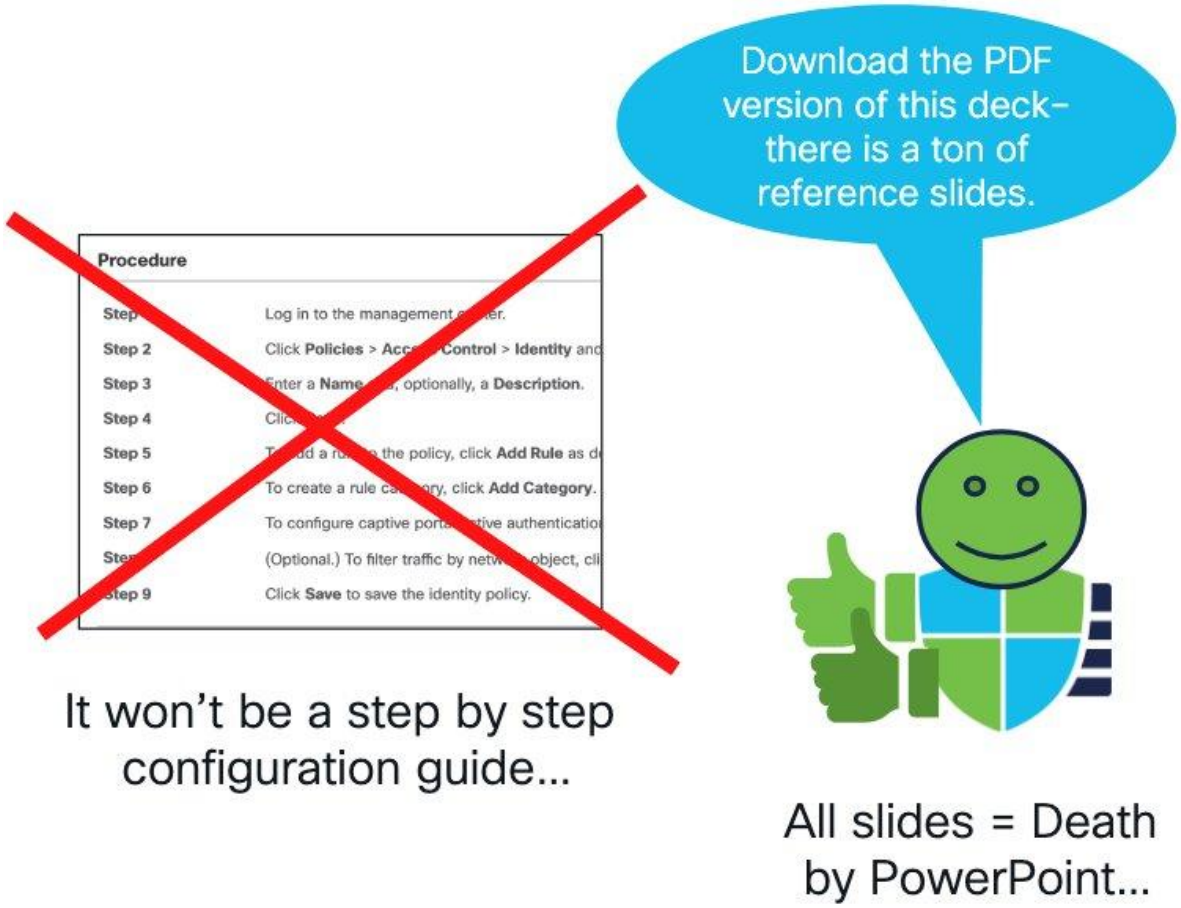
Principal Engineer – Security TAC

- 13+ Years of Security Experience
- Cisco Live Distinguished Speaker
- Snort Expert
- Sourcefire Veteran
- Automation Enthusiast
- 1 – Malware Detection Patent Holder

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Before We Begin Pact



© 2025 Cisco and/or its affiliates. All rights reserved.

Before We Begin Pact

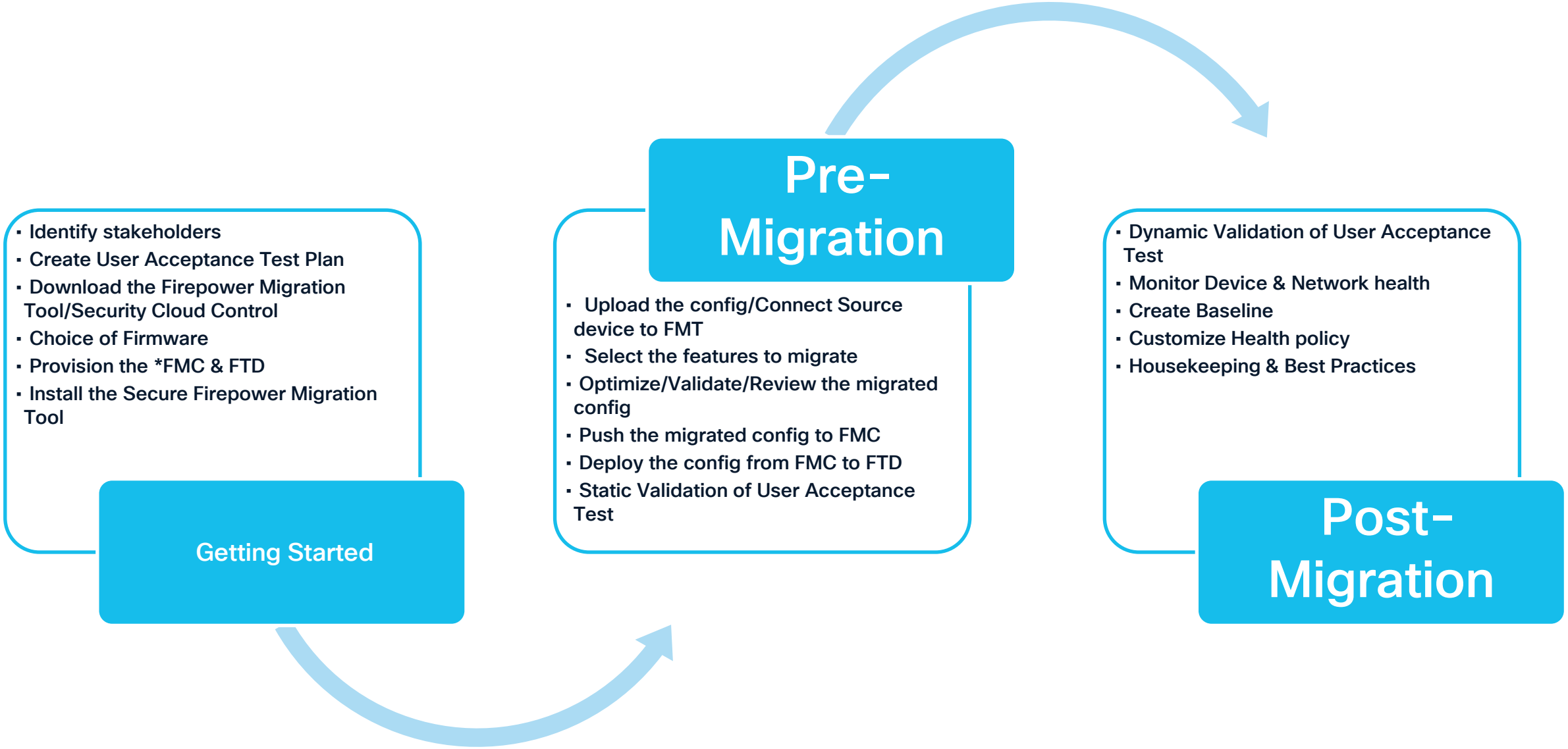
The content of this deck improves and evolves with your valuable feedback!

Put your email in the comment – I WILL respond ☺

© 2025 Cisco and/or its affiliates. All rights reserved.

Migration Lifecycle

Migration Workflow



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Getting Started

Behind the Scenes

01
Identify Stakeholders

02
Installation (FMC,FTD & FMT)

03
Software Conformance

04
Version Compatibility

05
Features Available

06
User Acceptance Test

© 2025 Cisco and/or its affiliates. All rights reserved.

Firepower Migration Tool

Firepower Migration Tool

Air gapped version available on demand

System & File Permissions

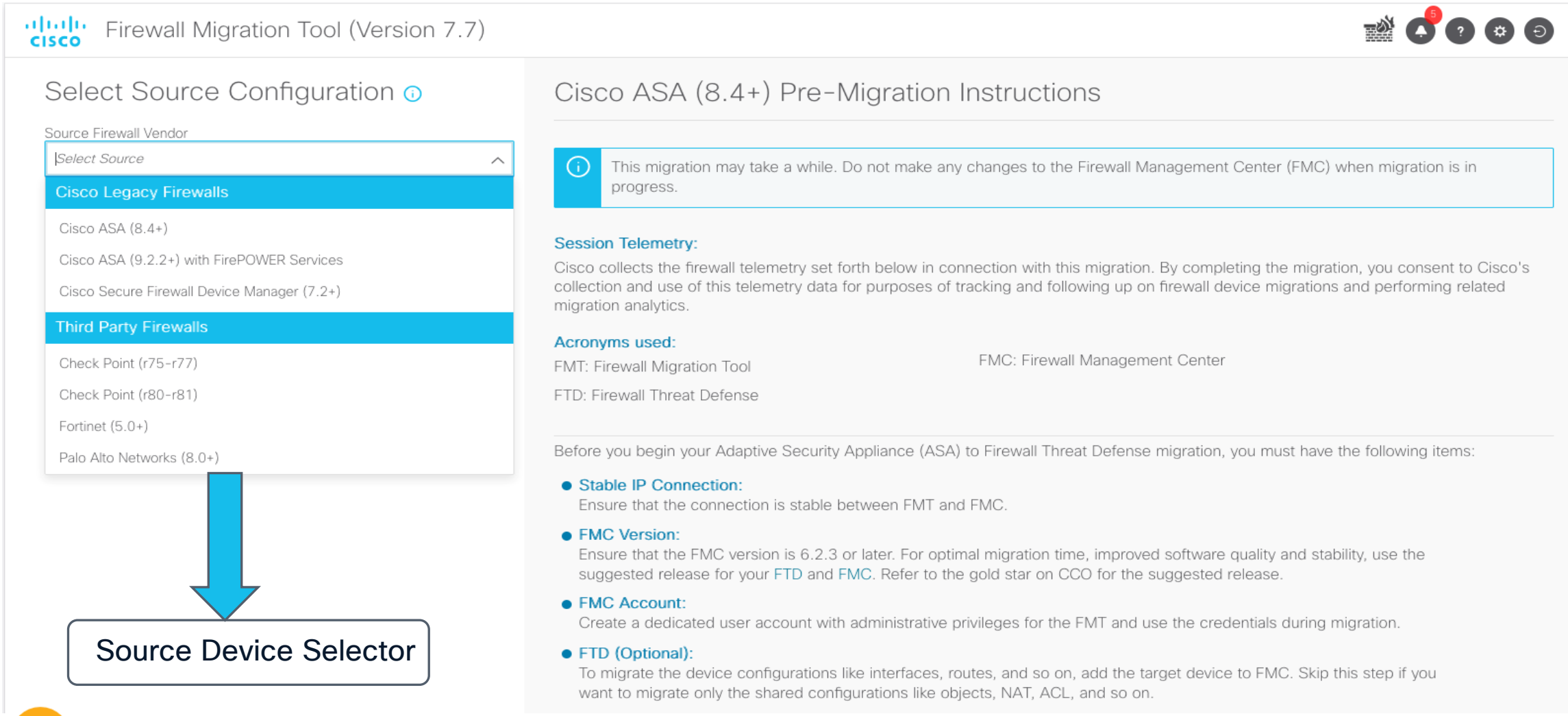
Pop-Up Blockers (Authentication in browser)

Always run the latest version of Firepower Migration Tool (Uninstall any older versions)

© 2025 Cisco and/or its affiliates. All rights reserved.

Pre-Migration Phase

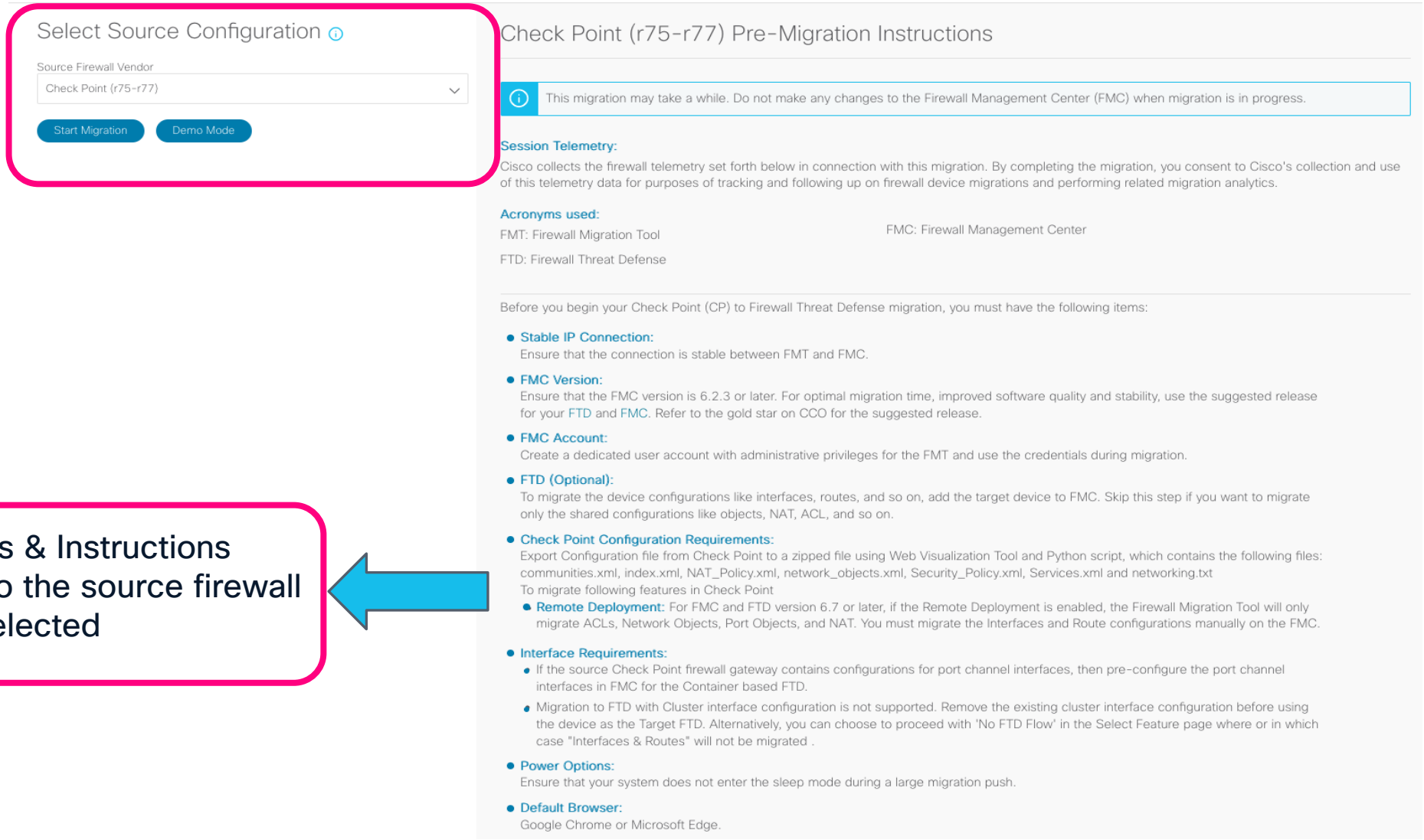
FMT Navigation



The console must stay open while the Secure Firewall Migration Tool is open and running

© 2025 Cisco and/or its affiliates. All rights reserved.

FMT Navigation

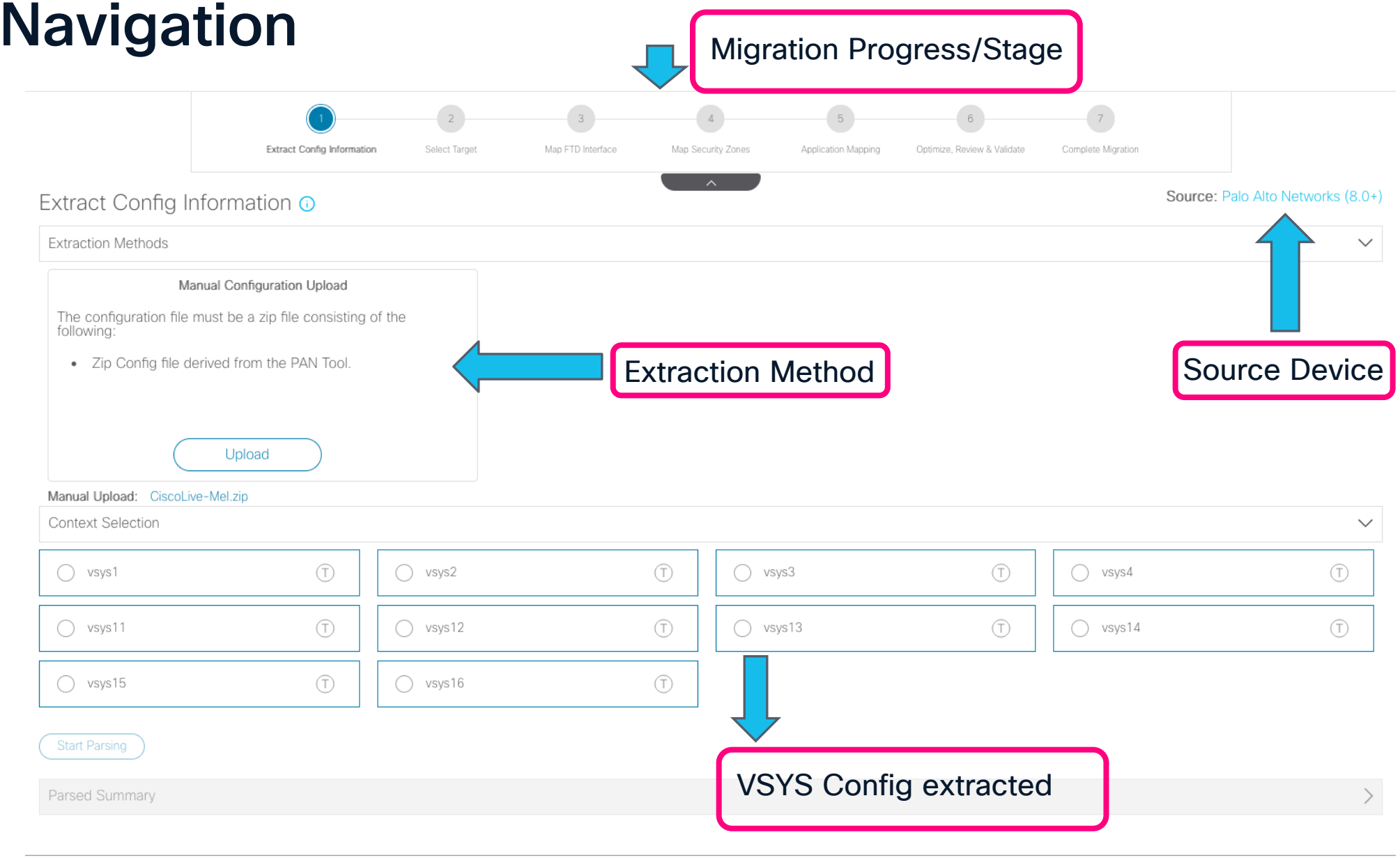


Guidelines & Instructions specific to the source firewall vendor selected

Ensure the right config extraction methods are used based on source device

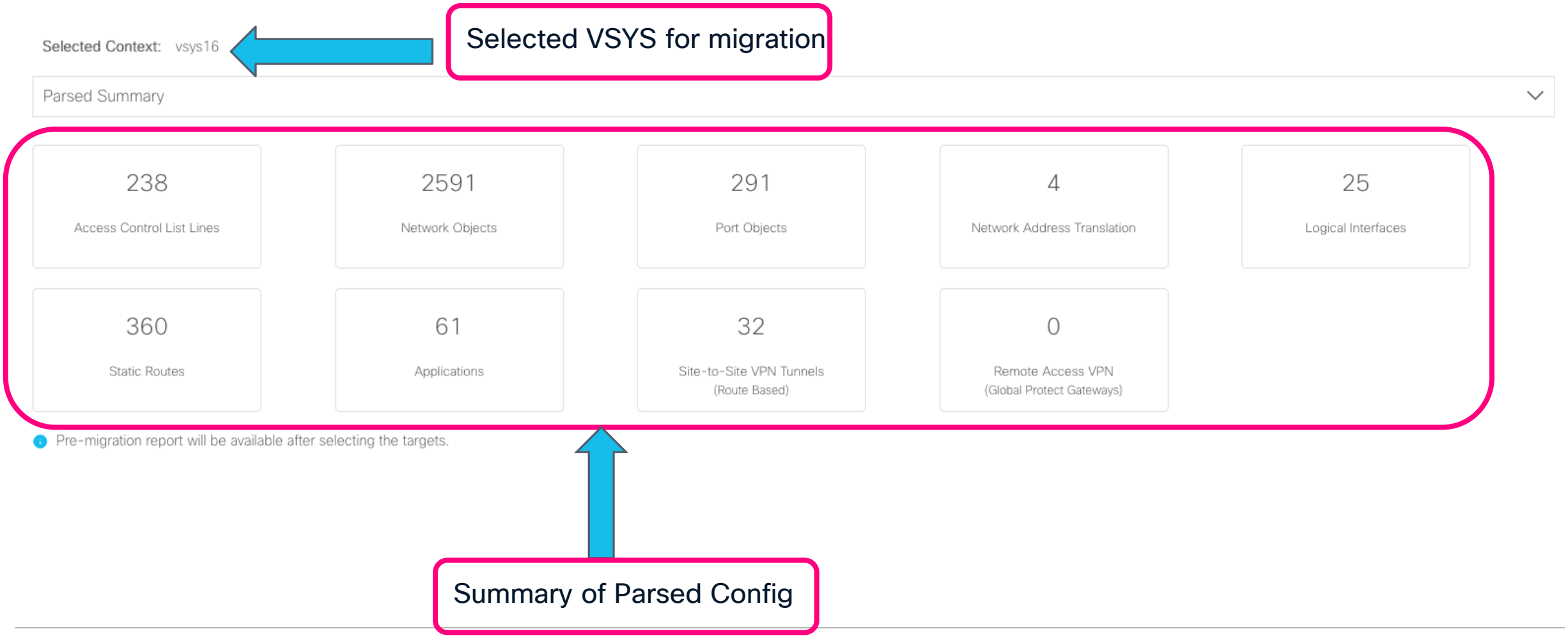
© 2025 Cisco and/or its affiliates. All rights reserved.

FMT Navigation



© 2025 Cisco and/or its affiliates. All rights reserved.

FMT Navigation



© 2025 Cisco and/or its affiliates. All rights reserved.

Pre-Migration Report

Overall Summary

- Summary of the config that is successfully migrated.
- Policy names, Rule counts, Objects, Logical interfaces, Applications, Static routes, VPN config etc.

Config lines with errors

- Information about configuration elements that couldn't be migrated successfully due to parsing issues by the FMT
- Network Objects, Routes etc. (Fix them and re-upload the config file from source device)

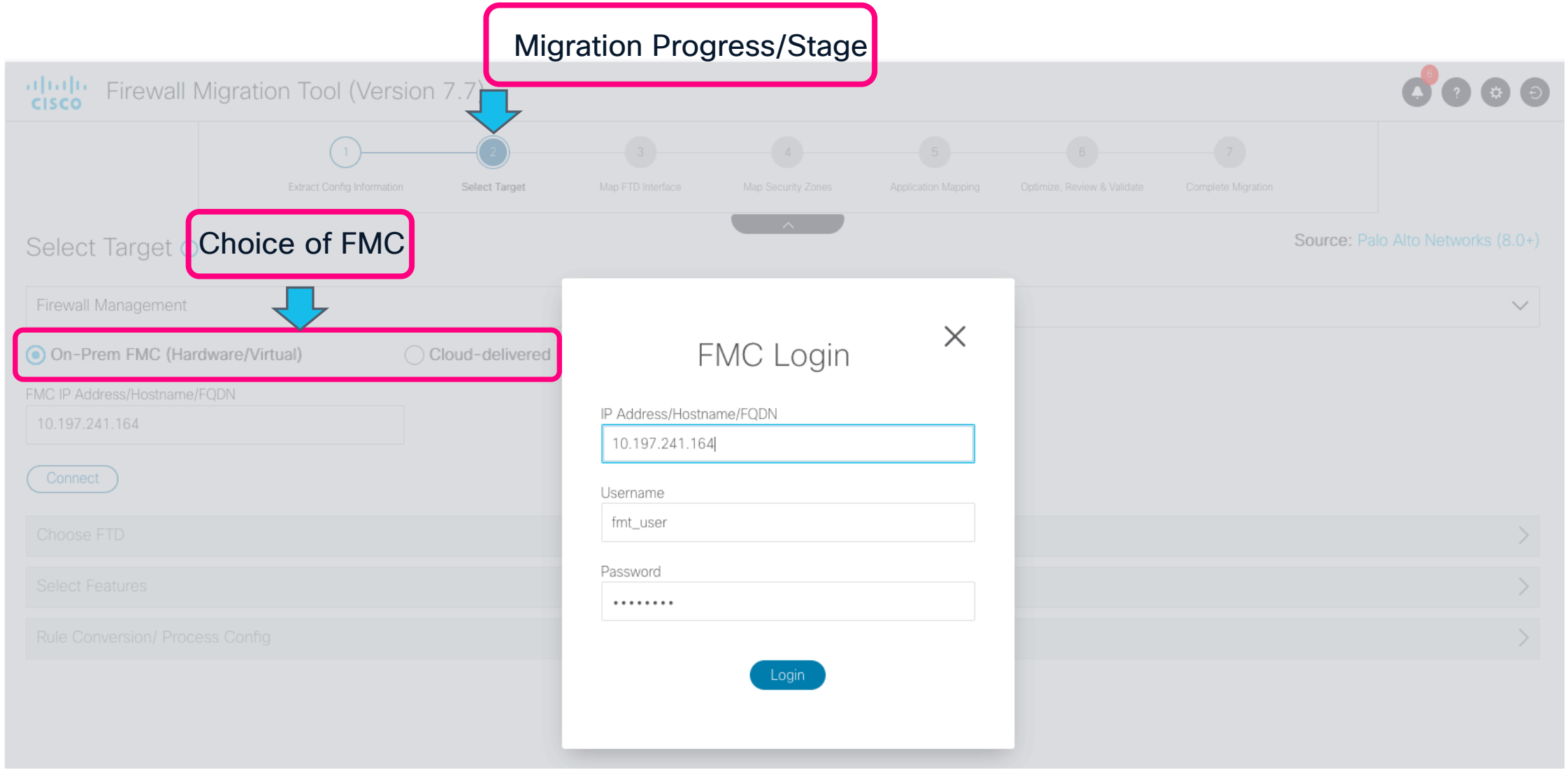
Ignored configurations

- List of all the configuration elements that are ignored by FMT during migration
- Review these lines, verify whether each feature is supported in FMC

Pre-Migration report provides insights into corrective actions if there are any errors identified in config

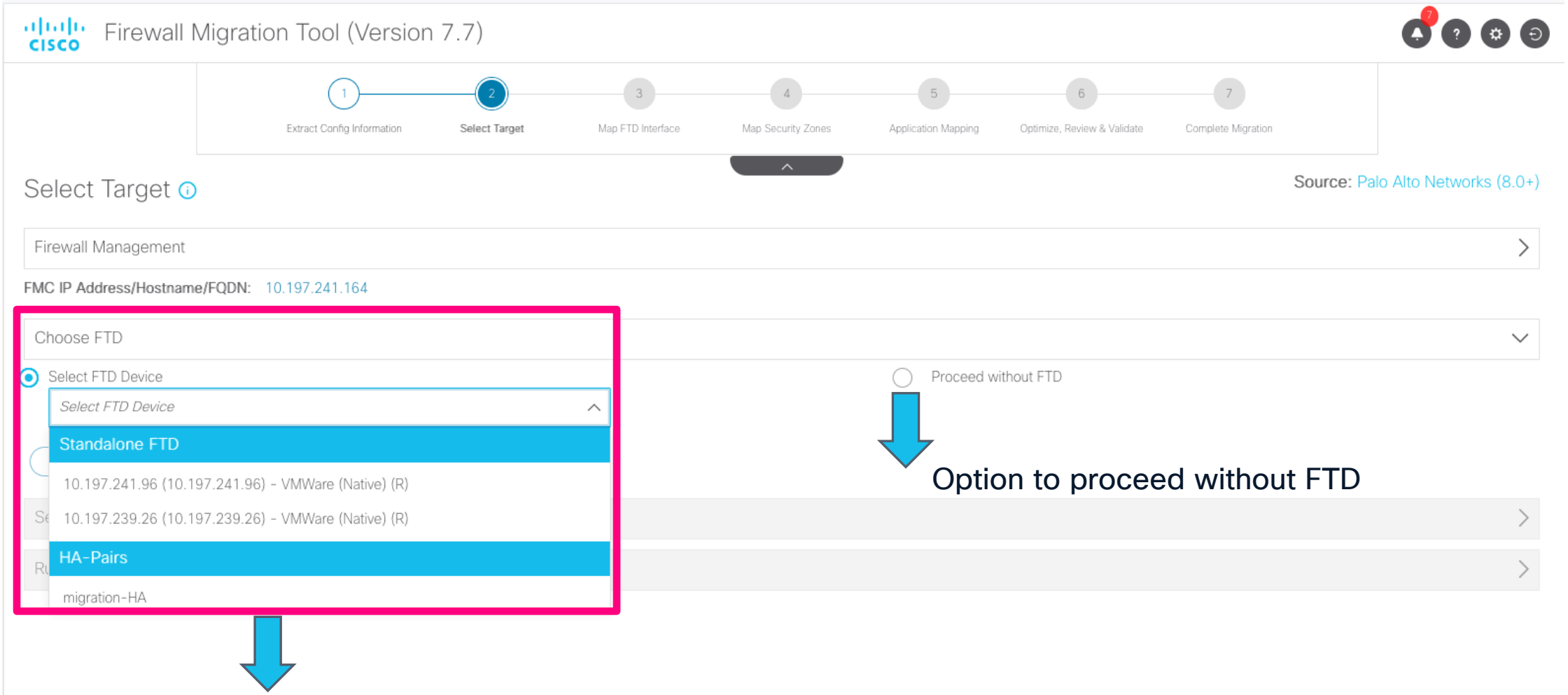
© 2025 Cisco and/or its affiliates. All rights reserved.

Target Selection



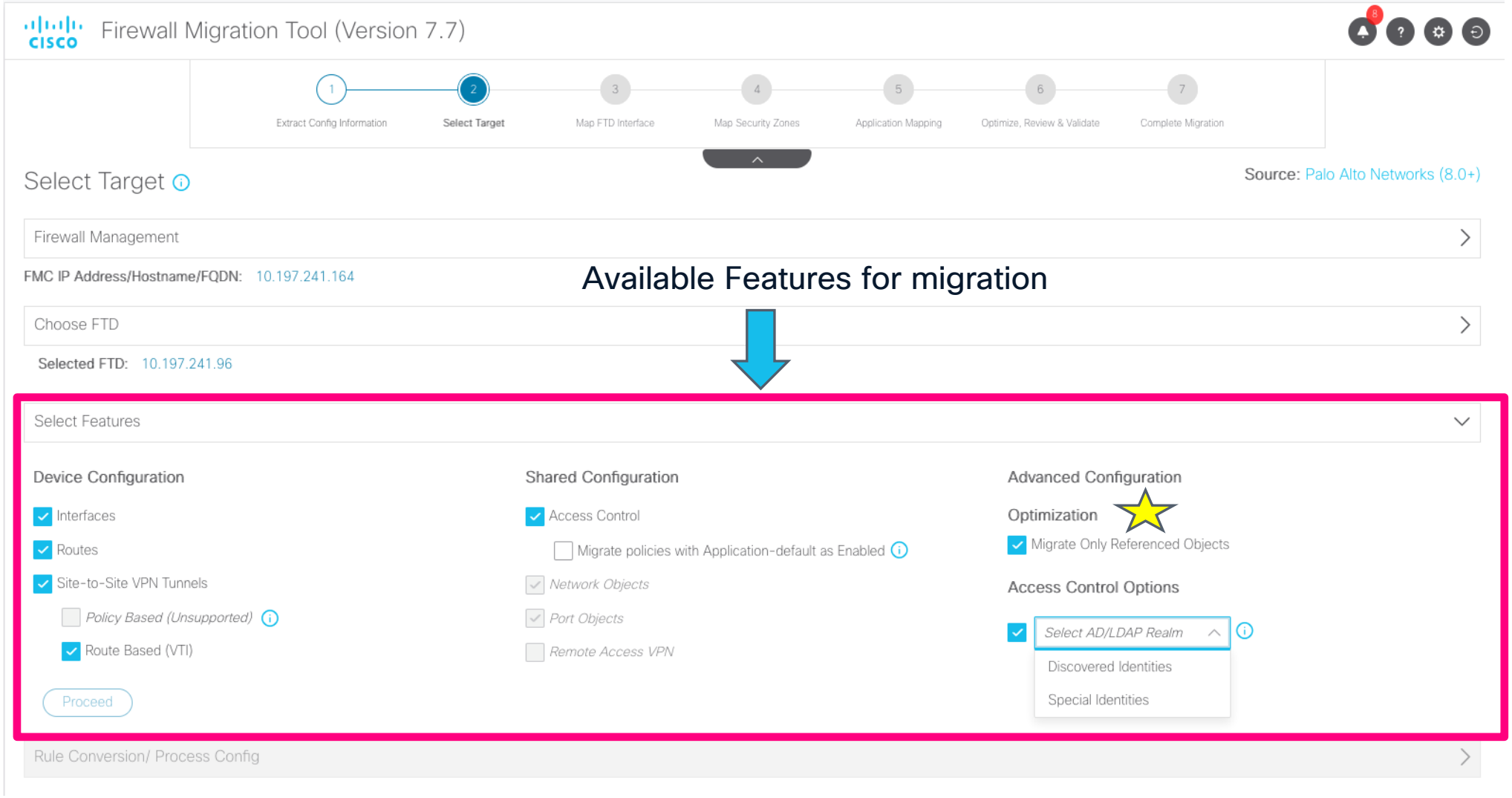
© 2025 Cisco and/or its affiliates. All rights reserved.

Target Selection



© 2025 Cisco and/or its affiliates. All rights reserved.

Feature Selection

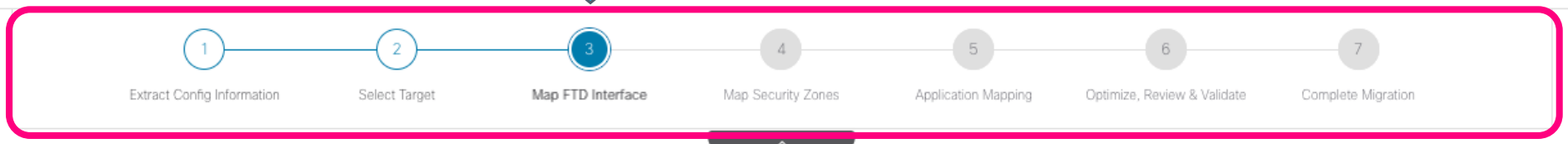


Enable this to ensure that unused objects are not migrated and only referenced one are migrated

© 2025 Cisco and/or its affiliates. All rights reserved.

Interface Mapping

Migration Progress/Stage



Map FTD Interface

Source: Palo Alto Networks (8.0+)
Target FTD: FTD-2-Instance-1

PAN Interface Name	FTD Interface Name	Mapped Nameif
ae1	Port-channel1	ae1
ae2		
ae2.3204	Ethernet1/1.10	ae2_3204
ae2.3205	Ethernet1/1.100	ae2_3205
ae3	Ethernet1/2	ae3
ae3.3200	Ethernet1/1.20	
ae3.3201	Ethernet1/1.30	ae3_3201
ae3.3202	Ethernet1/1.40	ae3_3202
ae3.3203	Ethernet1/1.50	ae3_3203
ae3.3299	Ethernet1/1.60	ae3_3299

Source Device Interface List

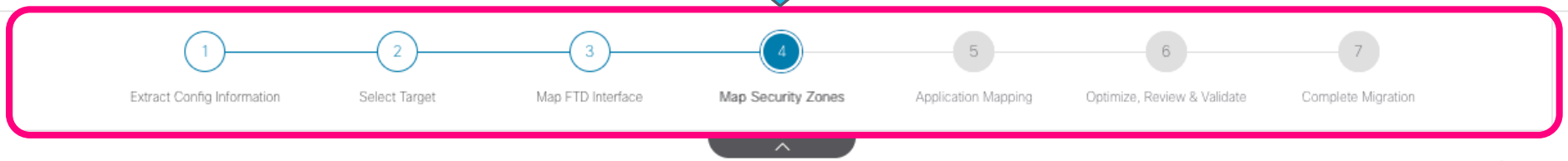
FTD Device Interface List

Ensure that number of interfaces on FTD is greater than or equal to Source Device interface

© 2025 Cisco and/or its affiliates. All rights reserved.

Zones Mapping

Migration Progress/Stage



Map Security Zones

Source: Palo Alto Networks (8.0+)
Target FTD: FTD-2-Instance-1

Add SZ | Auto-Create

PAN Zone Name	FMC Security Zones
Inside	Select Security Zone
Outside	Select Security Zone
DMZ	Select Security Zone
VPN	Select Security Zone
Prod	Select Security Zone
Staging	Select Security Zone
Servers	Select Security Zone
Guest	Select Security Zone

This would auto-create zones identical to Source Device Zones

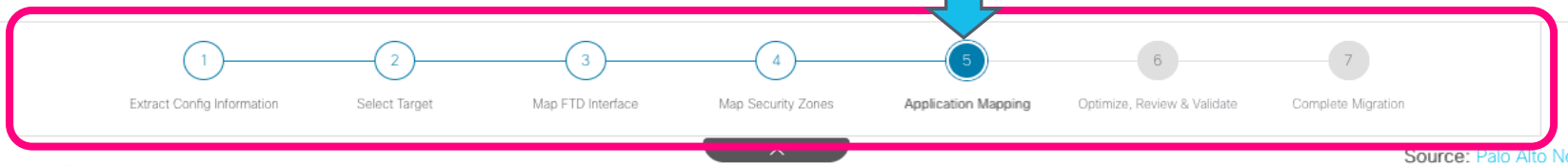
Manual zone creation

Note: Interfaces that are used in multiple configurations are allowed to have their unique security zones. The security zone mapping section for these interfaces will be greyed out.

© 2025 Cisco and/or its affiliates. All rights reserved.

Application Mapping (1/2)

Migration Progress/Stage



Application Mapping

Source: Palo Alto Networks (8.0+)

Target FTD: FTD-2-Instance-1

Valid Mappings (37/42) | Blank Mappings (5/42) | Invalid Mappings (0/42)

Valid Source Applications	Mapping Mode	Target Application/Ports
ms-netlogon	application	Netlogon
msrpc	application	DCE/RPC
rpc	application	ERPC
snmp-trap	application	SNMP trap (Deprecated)
windows-remote-management	application	Microsoft WSMan
traceroute	application	traceroute (Deprecated)
vmware	application	VMware vCenter client,VMware Fault Domain Manager, VMWare Remote Authentication, VMware Horizon View, VMware Server Console
ssl	application	SSL
active-directory	application	AD DSAOP
dns	application	DNS

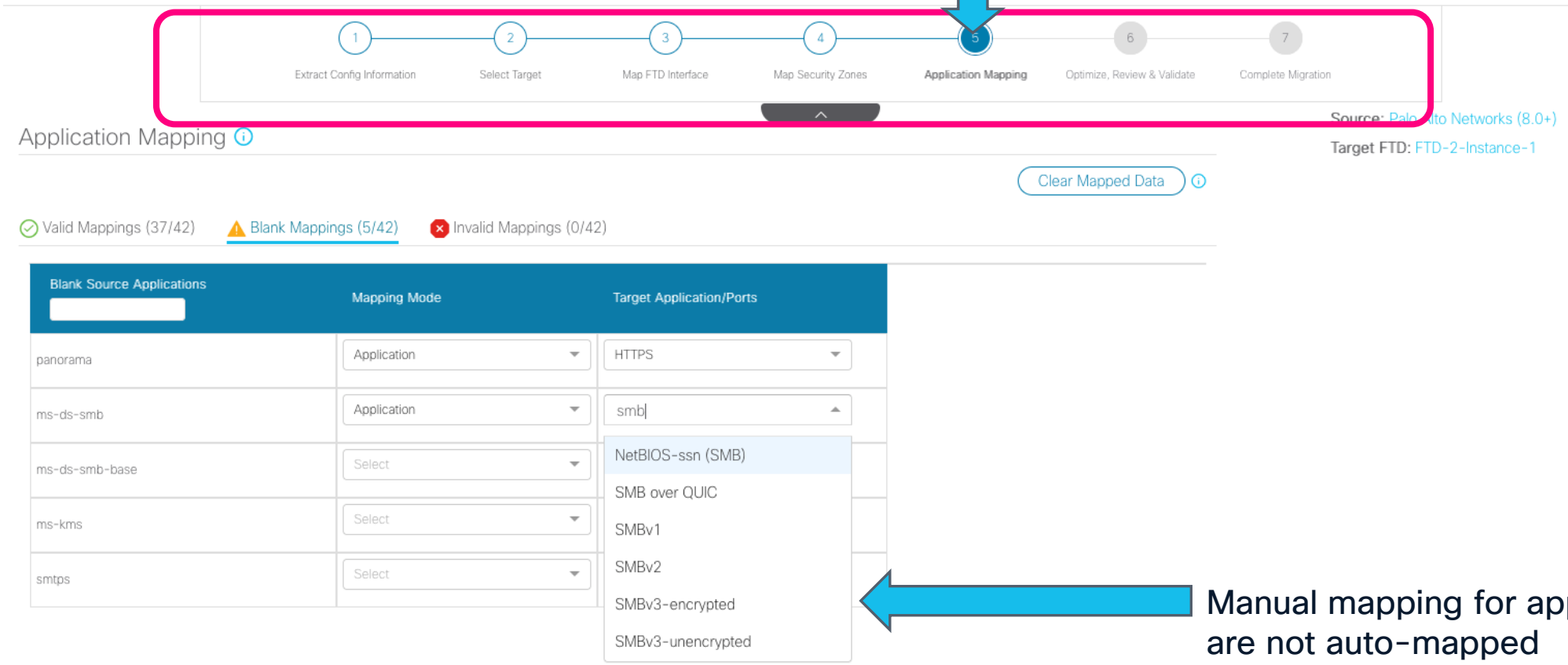
Auto Mapping of Applications

10 per page 1 to 10 of 37 Page 1 of 4

© 2025 Cisco and/or its affiliates. All rights reserved.

Application Mapping (2/2)

Migration Progress/Stage



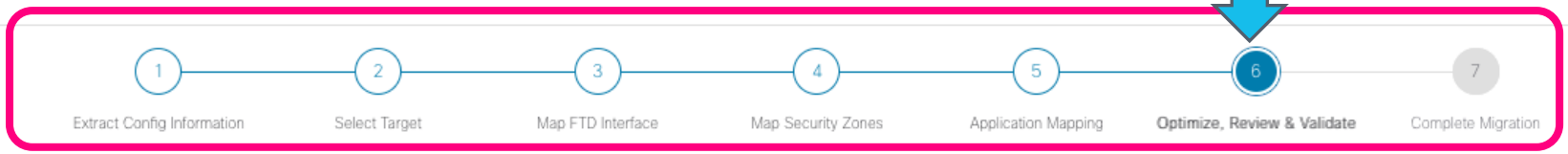
Manual mapping for apps that are not auto-mapped

Complete list of applications is available at https://appid.cisco.com/

© 2025 Cisco and/or its affiliates. All rights reserved.

Optimize, Review & Validate

Migration Progress/Stage



Optimize, Review and Validate Configuration

Source: Palo Alto Networks (8.0+)
Target FTD: FTD-2-Instance-1

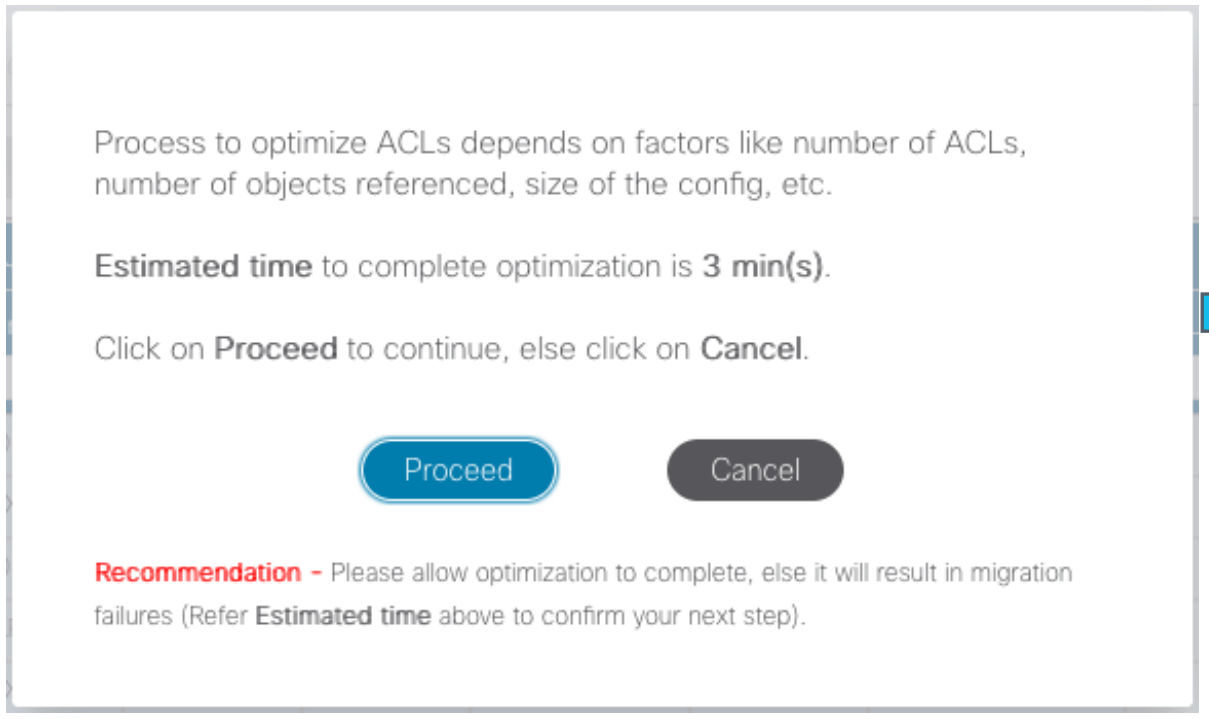
Access Control | Objects | NAT | Interfaces | Routes | Site-to-Site VPN | Remote Access VPN

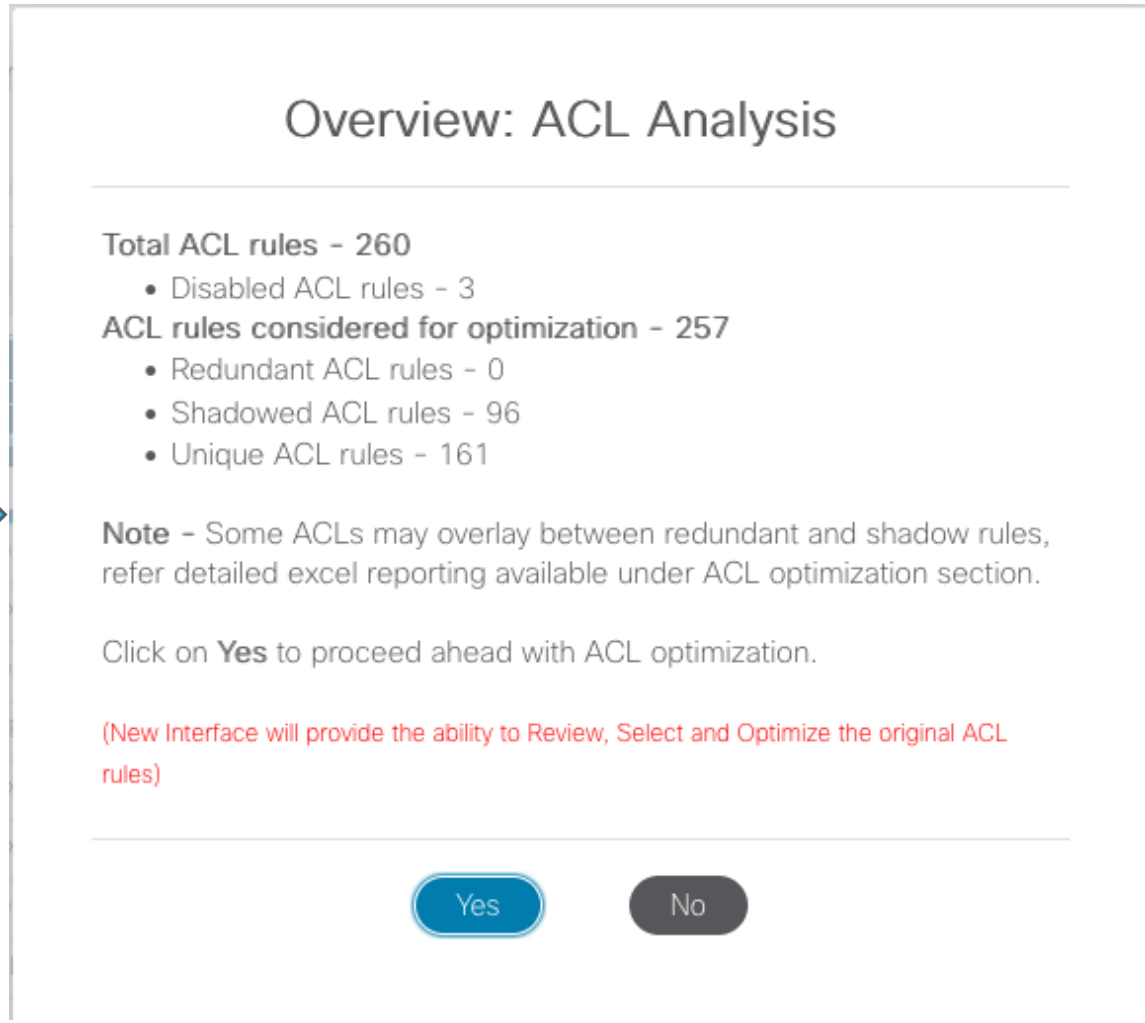
Select all 260 entries | Selected: 260 / 260 | Actions | Save | Search

			SOURCE			DESTINATION							TIME BASED
	#	Name	Zone	Network	Port	Zone	Network	Port	Application	URLs	State	Action	Objects
☑	1		ANY		ANY	ANY		Ping	ANY	NA		Allow	None
☑	2		ANY		ANY	ANY		ANY	syslog	NA		Allow	None
☑	3		ANY		ANY	ANY		SYSLOG_PR...	ANY	NA		Allow	None
☑	4		ANY		ANY	ANY		ANY	SSH, SNMP	NA		Allow	None
☑	5		ANY		ANY	ANY		ANY	SNMP	NA		Allow	None
☑	6		ANY		ANY	ANY		ANY	Netflow	NA		Allow	None
☑	7		ANY		ANY	ANY		ANY	NTP, DNS	NA		Allow	None
☑	8		ANY		ANY	ANY		NETBKP_AP...	ANY	NA		Allow	None
☑	9		ANY		ANY	ANY		ANY	Microsoft System C...	NA		Allow	None
☑	10		ANY		ANY	ANY		SCCM_PRIV...	ANY	NA		Allow	None

© 2025 Cisco and/or its affiliates. All rights reserved.

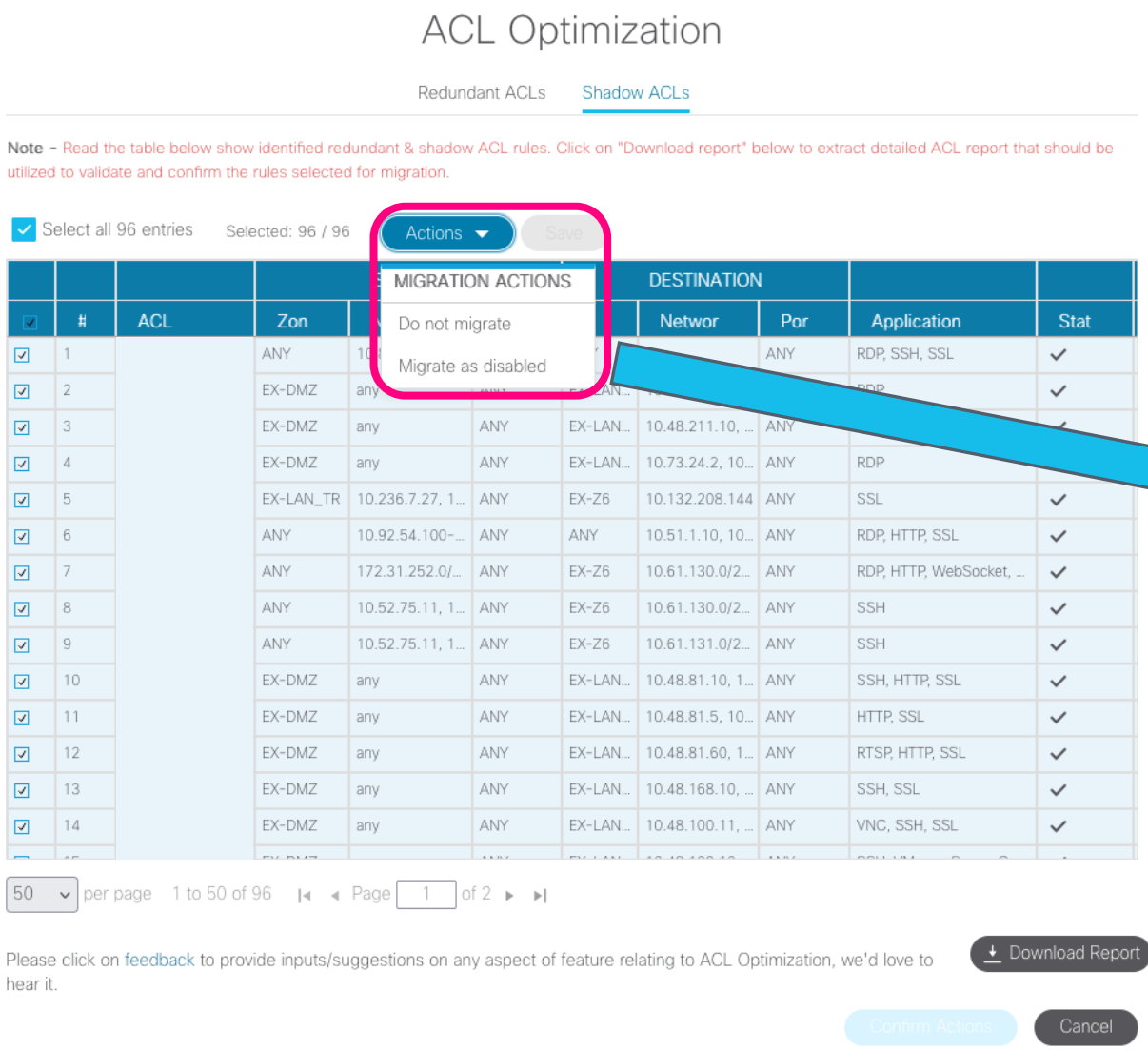
Analysis





© 2025 Cisco and/or its affiliates. All rights reserved.

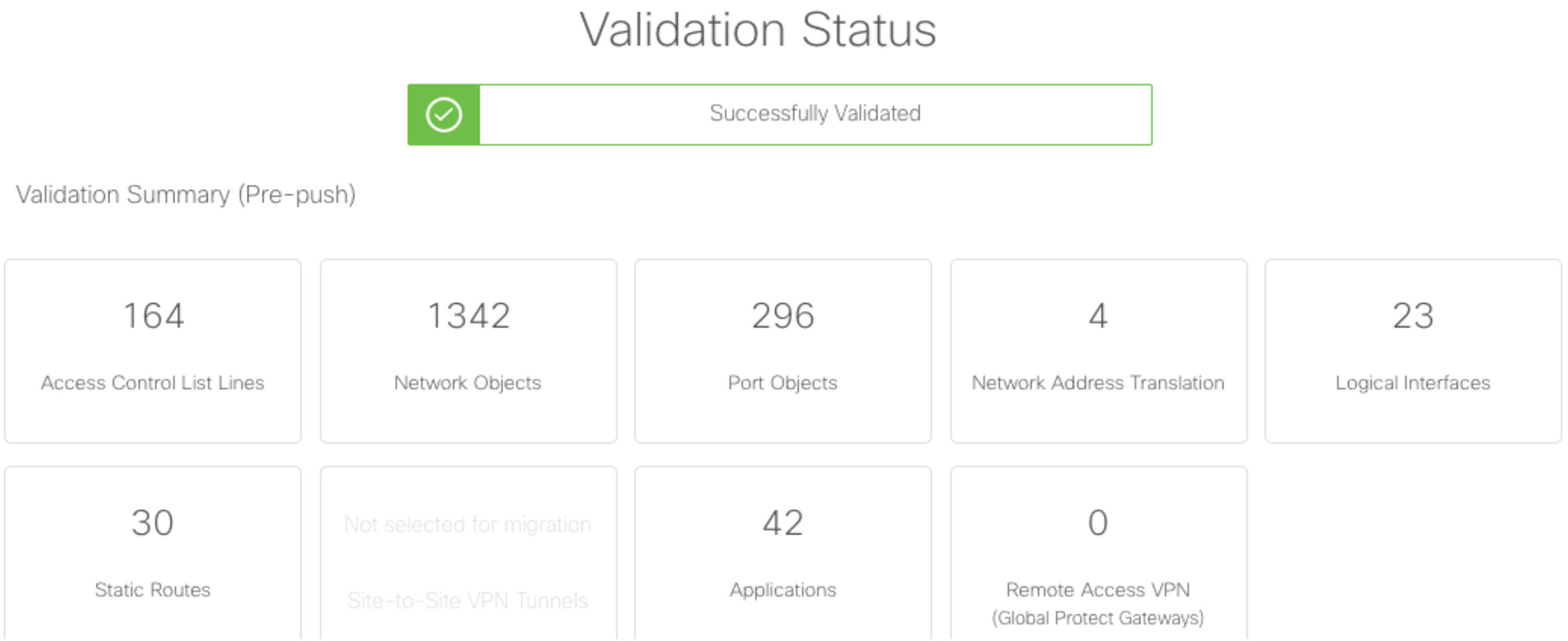
Optimization Actions



- **Do not migrate :** Rules are not pushed to FMC
- **Migrate as disabled:** Rules are pushed to FMC but marked as disabled, this means it will not be deployed to FTD

© 2025 Cisco and/or its affiliates. All rights reserved.

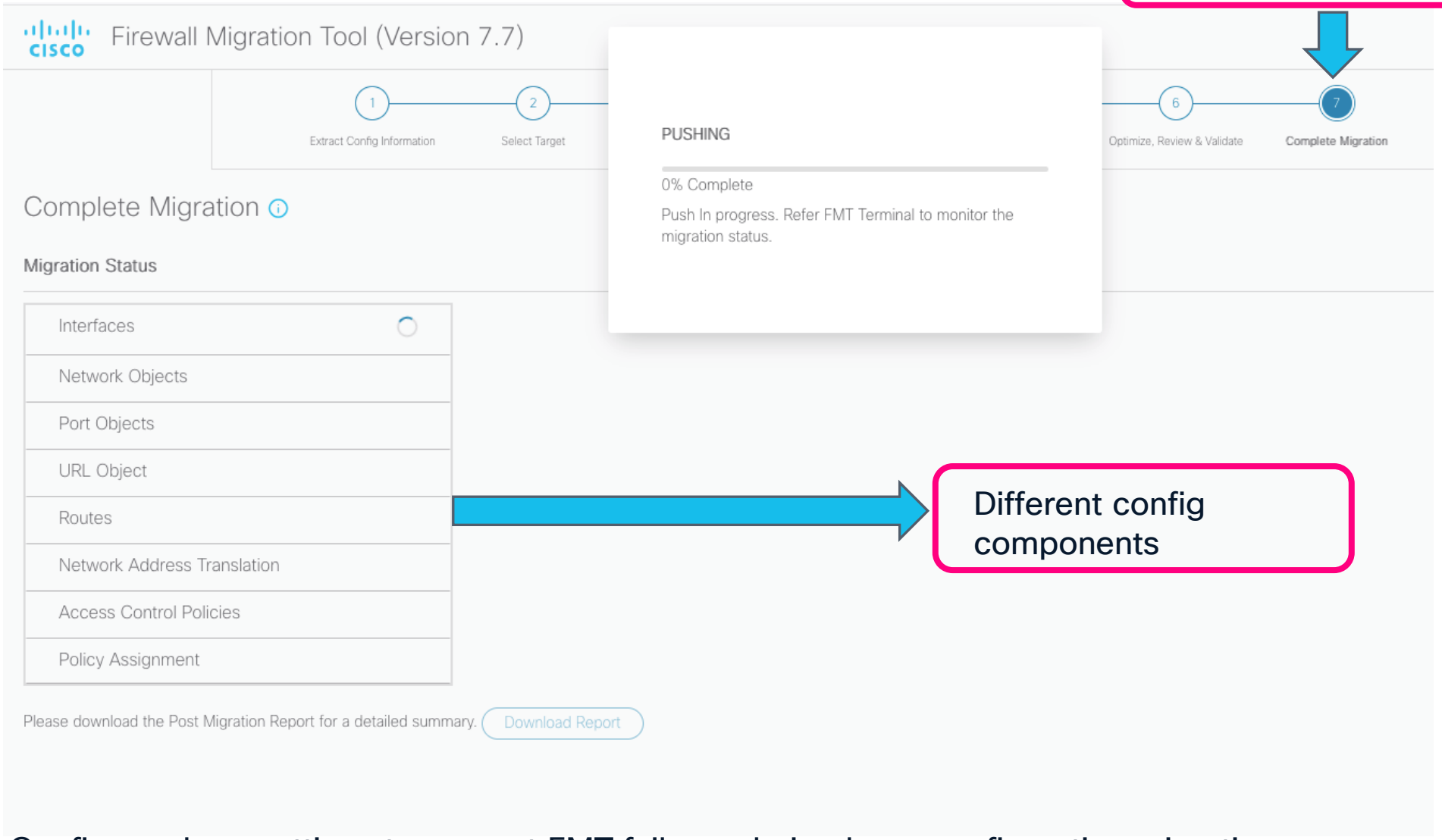
Summary



© 2025 Cisco and/or its affiliates. All rights reserved.

Config Push

Migration Progress/Stage



Different config components

Configure sleep settings to prevent FMT failures during large configuration migration

© 2025 Cisco and/or its affiliates. All rights reserved.

Post-Migration Report

Migration Summary

- Configuration that are successfully migrated.
- Useful to compare with pre-migration report for differences.

Selective Policy Migration

- Details of feature selected for migrations

Migration Conversions

- Network/Service object handling
- Partially migrated & Unsupported configurations with reasons
- Expanded Access Control Rules

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Validations

Static & Dynamic Validations

Static Checks

- Packet tracer
- Policy Analyzer Optimizer
- Best Practice Recommendations
- System Health
- Baseline

Dynamic Checks

- Elephant Flow Detection
- Configured Traffic Blocks
- System Health
- Application Performance
- Baseline

- Update any static routes which refer to the IP address (If IP address scheme is changed)
- For dynamic routing protocols, ensure that neighbors see FTD IP as the next hop for expected destinations
- Clear the Address Resolution Protocol (ARP) cache on the surrounding switching infrastructure

© 2025 Cisco and/or its affiliates. All rights reserved.

Firepower Device Migration

What's Shipping

FMC 7.4.0

Source
- 11XX: 1120, 1140 & 1150
- 21XX: 2110, 2120, 2130 & 2140

Target
- 31XX: 3105, 3110, 3120, 3130 & 3140

FMC 7.6.1

New Source
- 41XX: 4110, 4120, 4140 & 4150 (M4 Blades)
- 93XX: SM24, SM36 & SM44 (M4 Blades)

Target
- New 42XX Series: 4215, 4225 & 4245

FMC 10.0.0

New Source
- 41XX Series: 4112, 4115, 4125 & 4145 (M5 Blades)
- 9300 Series: SM40, SM48 & SM56 (M5 Blades)
- 1010 Series

Target
- New 12XX Series: 1210CE, 1210CP & 1210CX
- New 61XX Series: 6160 & 6170
- New 220 Series

All the source and target devices are forward compatible

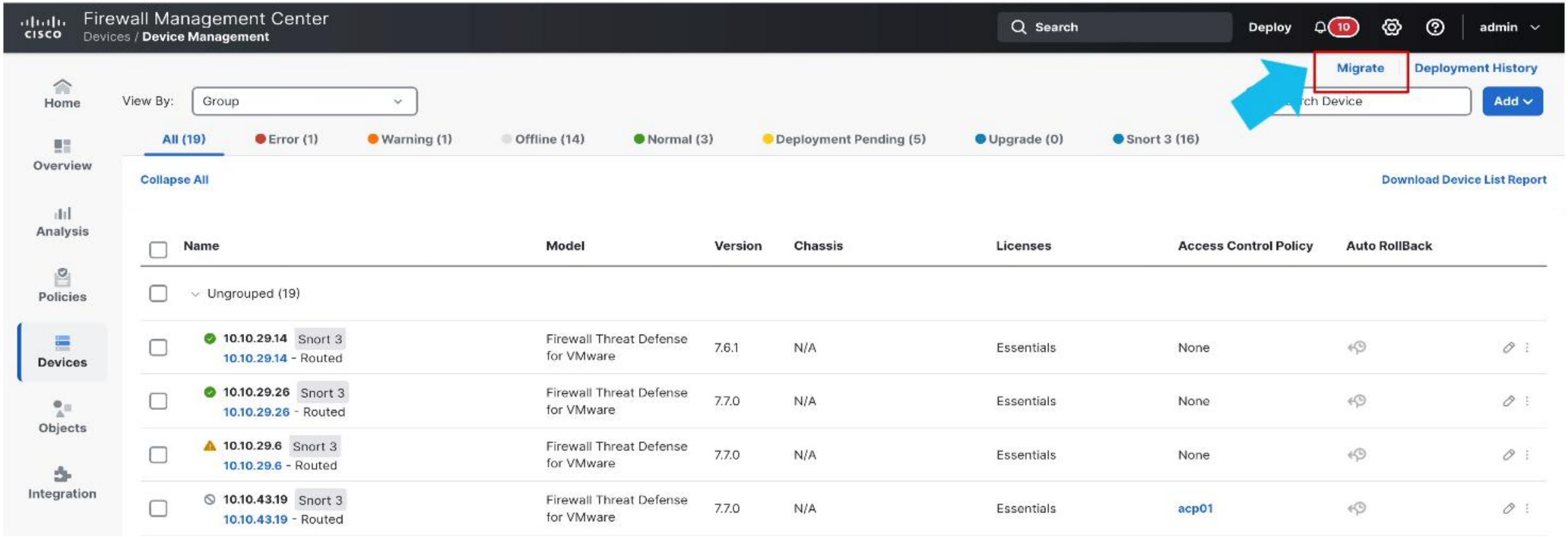
© 2025 Cisco and/or its affiliates. All rights reserved.

Before We Begin

- Registered to same FMC(domain)
- No active tasks (Deployments, domain movement, import/export)
- Change the IP addresses of the interfaces if the source device is live, as they are copied to the target device from the source device.
- Update NAT policies with the modified IP addresses.
- Re-enroll the device certificates, if any, on the target device.
- Configure HA parameters such as monitored interfaces, failover trigger criteria, and interface MAC addresses.
- Configure the diagnostic interface as it gets reset after migration.
- Configure SNMP using the platform settings for the device.

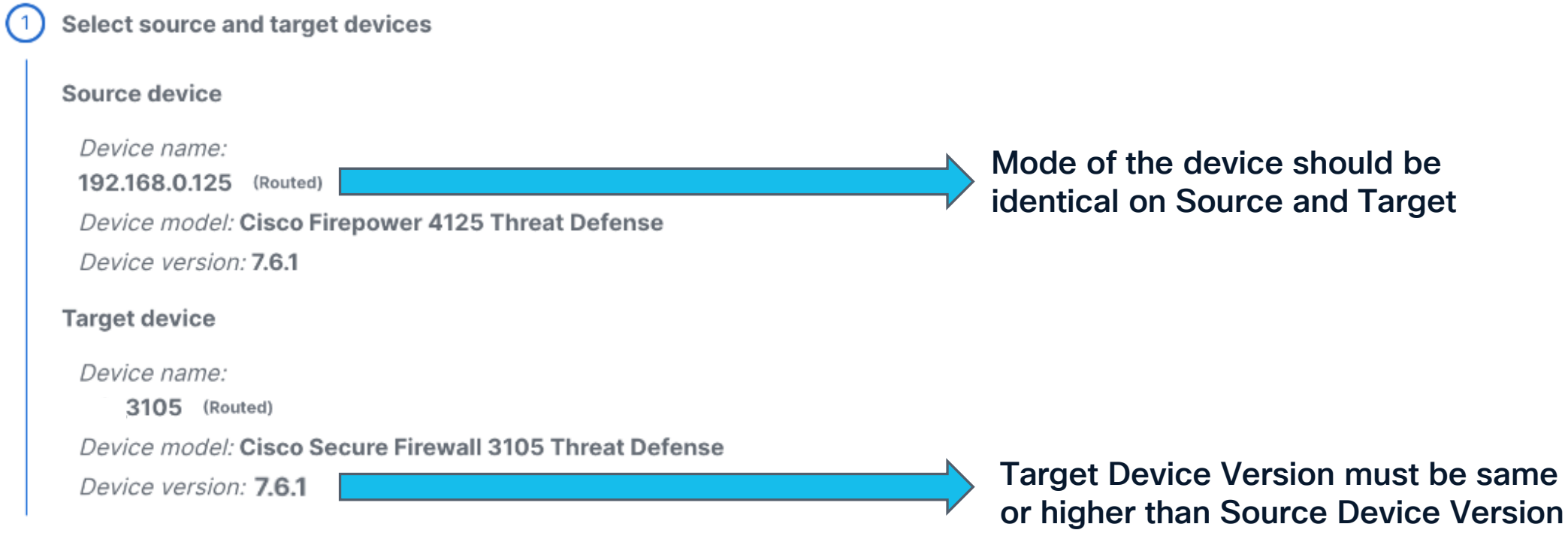
© 2025 Cisco and/or its affiliates. All rights reserved.

Getting Started



© 2025 Cisco and/or its affiliates. All rights reserved.

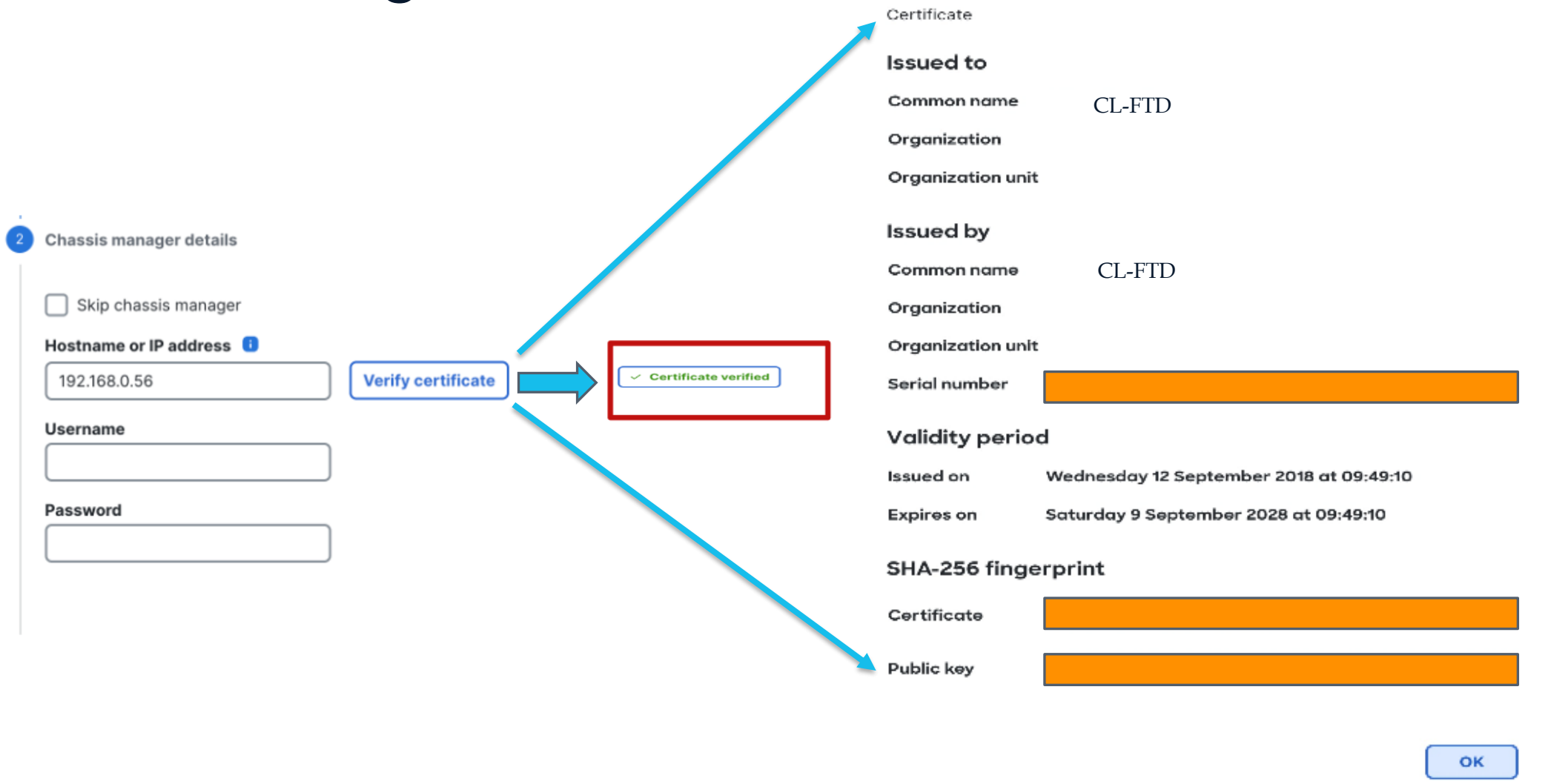
Device Selection



Forward Error Correction is available on 25G/100G interfaces on 31XX/42XX platforms

© 2025 Cisco and/or its affiliates. All rights reserved.

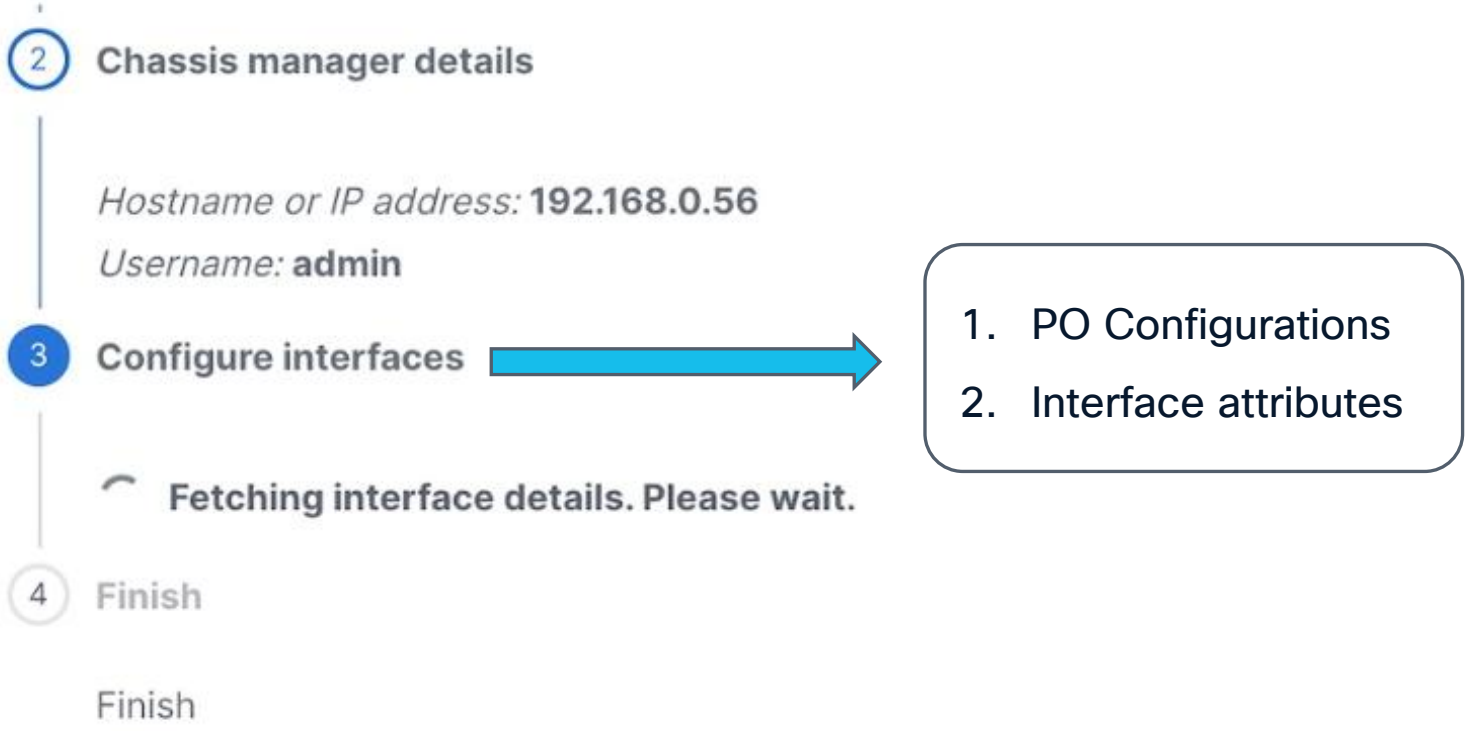
Chassis Manager Details



This step is applicable for 4100/9300 devices to extract config done from chassis manager

© 2025 Cisco and/or its affiliates. All rights reserved.

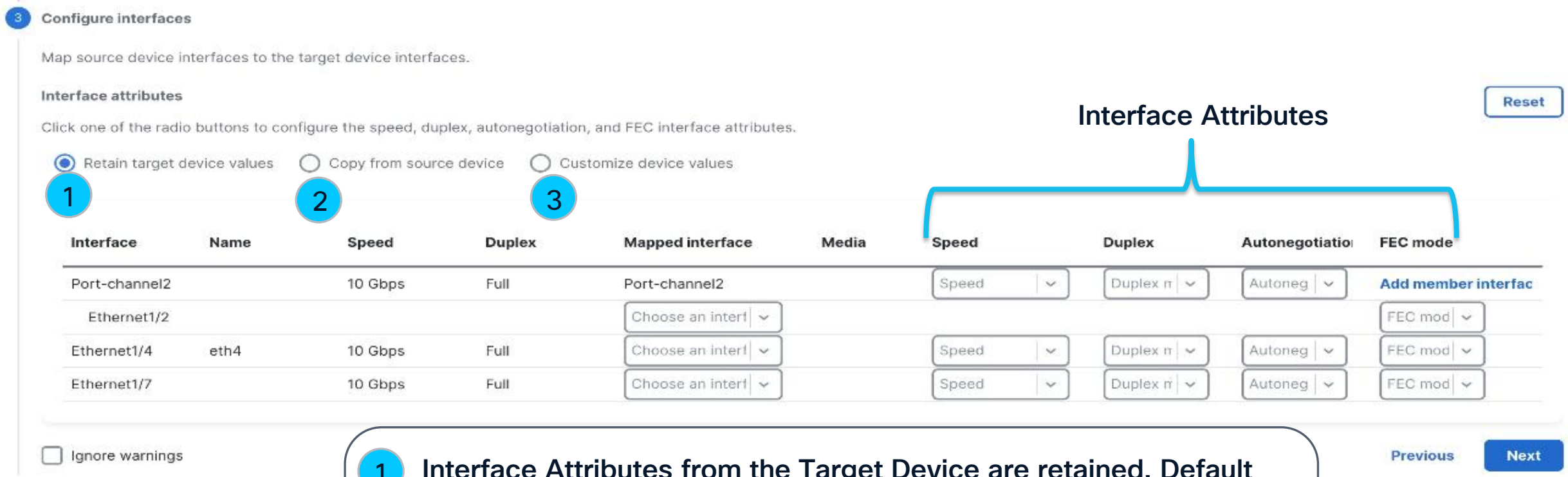
Chassis Manager Details



1. PO Configurations
2. Interface attributes

© 2025 Cisco and/or its affiliates. All rights reserved.

Interface Mapping



1. Interface Attributes from the Target Device are retained. Default Option
2. Interface Attributes are copied from Source to Target Device
3. Interface Attributes are customized from their default settings

Speed, duplex, and auto negotiation values are set to default if copied values are incompatible

© 2025 Cisco and/or its affiliates. All rights reserved.

Interface Mapping Summary

3 Configure interfaces

Interface attributes: User-provided values

Interface	Name	Speed	Duplex	Mapped interface	Media	Speed	Duplex	Autonegotiatio	FEC mode
Port-channel2		10 Gbps	Full	Port-channel2		10 Gbps	Full	False	
Ethernet1/2				Ethernet1/6	SFP				auto
Ethernet1/4	eth4	10 Gbps	Full	Ethernet1/4	SFP	10 Gbps	Full	False	auto
Ethernet1/7		10 Gbps	Full	Ethernet1/7	SFP	10 Gbps	Full	False	auto

4 Finish

Previous Submit

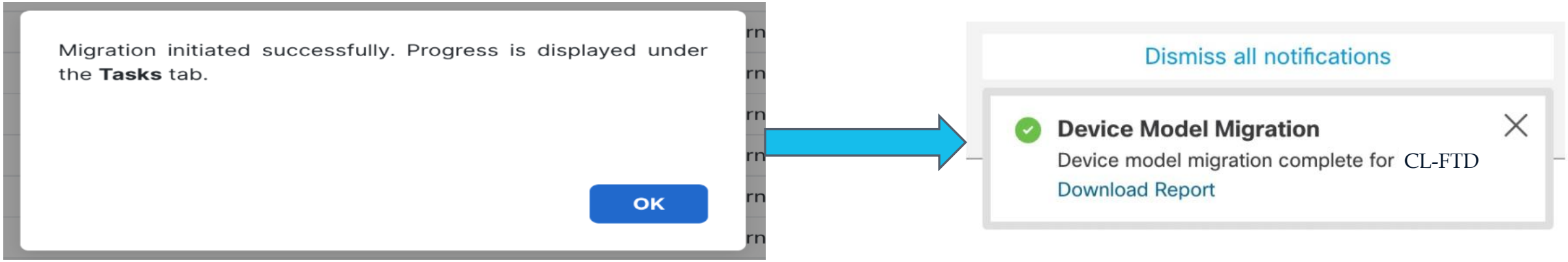
Only Data interfaces are listed for interface mapping

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Migrate

1. Post reviewing the interface summary. Proceed with “Submit”
2. Click “Submit” to initiate the migration task
3. Progress can be monitored through task notification
4. Once completed, user is notified along with “Download Report” option



The device will not be automatically deployed as part of the process; it will just be configured

© 2025 Cisco and/or its affiliates. All rights reserved.

FMC Migration

On-Prem Model Migration

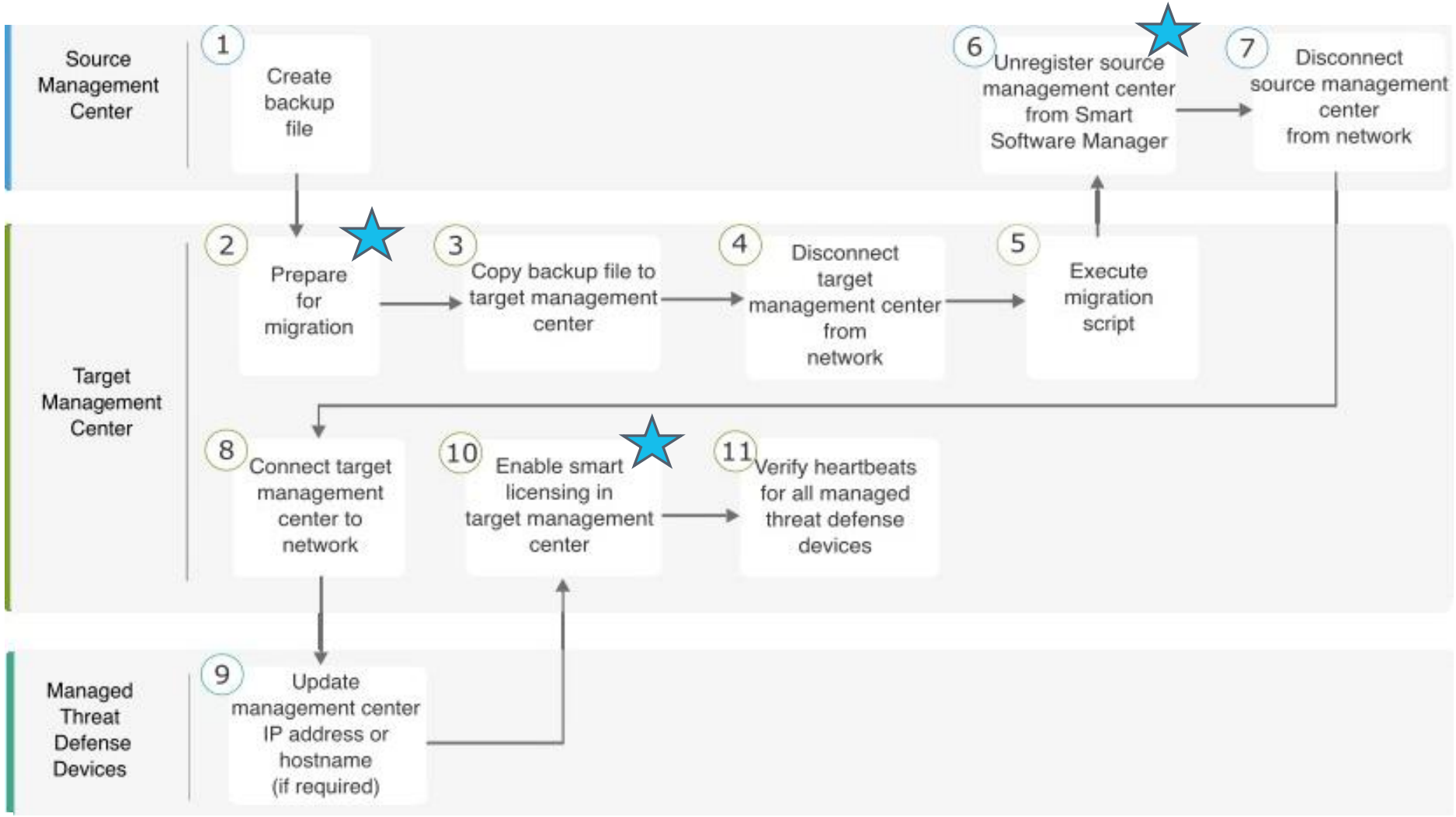
Prepare for Migration

- Target FMC should not have managed devices
- Target FMC should not be a part of High availability
- FTD registration, Deployment, & Backup should not be running during migration
- Supported migration path from the source to target FMC
- Classic license is not available for FMC Version 7.6+,as NGIPS is not supported
- Backup Availability

Model Migration Path: *Supported Paths*

© 2025 Cisco and/or its affiliates. All rights reserved.

Migration Workflow (Pre 10.0.0)



Before model migration, you must delete existing classic licenses.

© 2025 Cisco and/or its affiliates. All rights reserved.

Migration Script

- Log in to the target management center CLI.
- Run the expert command to switch to expert mode.
- Execute the migration command:

  /var/sf/bin/sf-migration.pl backup_file_path

- Example:

root@firepower:# /var/sf/bin/sf-migration.pl /var/sf/backup/source_local_backup

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Post Migration Activities

- From Version 7.4.x, update the following parameters, as needed:
  - IP address of the target FMC.
  - If the IP address of the FMC changes, edit the FMC Address in the threat defense devices.

    *This is not required if the management center can reach the threat defense device.

- Licensing
  - Smart Licensing: Deregister the licenses from the source FMC and register the licenses in the target FMC.
  - Classic license: Contact TAC to regenerate the license using the new MAC address of the FMC.

- After migration, if you want to manage a different group of FTD in the source FMC:
- Ensure that source FMC cannot reach the stale FTD.
- Delete the stale FTD that are now managed by the target FMC

© 2025 Cisco and/or its affiliates. All rights reserved.

Migrating to Public Cloud

- Use reserved static public IP addresses instead of default public IP addresses.
- Use FQDN/DNS name because it can be moved across the public IP addresses.
- If you do not want to update the public IP address of the target management center virtual, run the following command in the threat defense device CLI:

  configure manager add DONTRESOLVE any_key any_key_for_nat_field_input

- Before you run the above command, ensure that the management center virtual can connect to the threat defense device.
- If you do not perform the above operations, you must update the management center virtual IP address on the threat defense device using the following command in the threat defense device CLI:

  configure manager edit fmc_uuid displayname fmc_ipaddress

© 2025 Cisco and/or its affiliates. All rights reserved.

TAC Insights

Category	Error Message	Remediation
Hardware/Software	1. No migration path exists 2. Interface count mismatch 3. Migration data size is greater than the storage space of the target management center 4. Software version, SRU, LSP and VDB mismatch	1. Migration path not supported 2. Source & Target should have same number of interface 3. Increase the size of target management center 4. Ensure software conformance
Licenses	1. Device count is more than XXX 2. Out of compliance 3. Unable to communicate to licensing server	1. Licenses for managed device is less. 2. Insufficient licenses/unable to connect to licensing server 3. Connectivity issue (Proxy connection)
Connectivity	1. Devices not registered after migration 2. Devices show disabled on FMC 3. Policy Deploy failures	1. Check port requirements on 8305 2. IP and Port connectivity from target FMC 3. SFTunnel connectivity (8305)
Backup/Restore Failures	1. Database corruption 2. Version mismatch	1. Reach out to TAC for assistance 2. Software Conformance

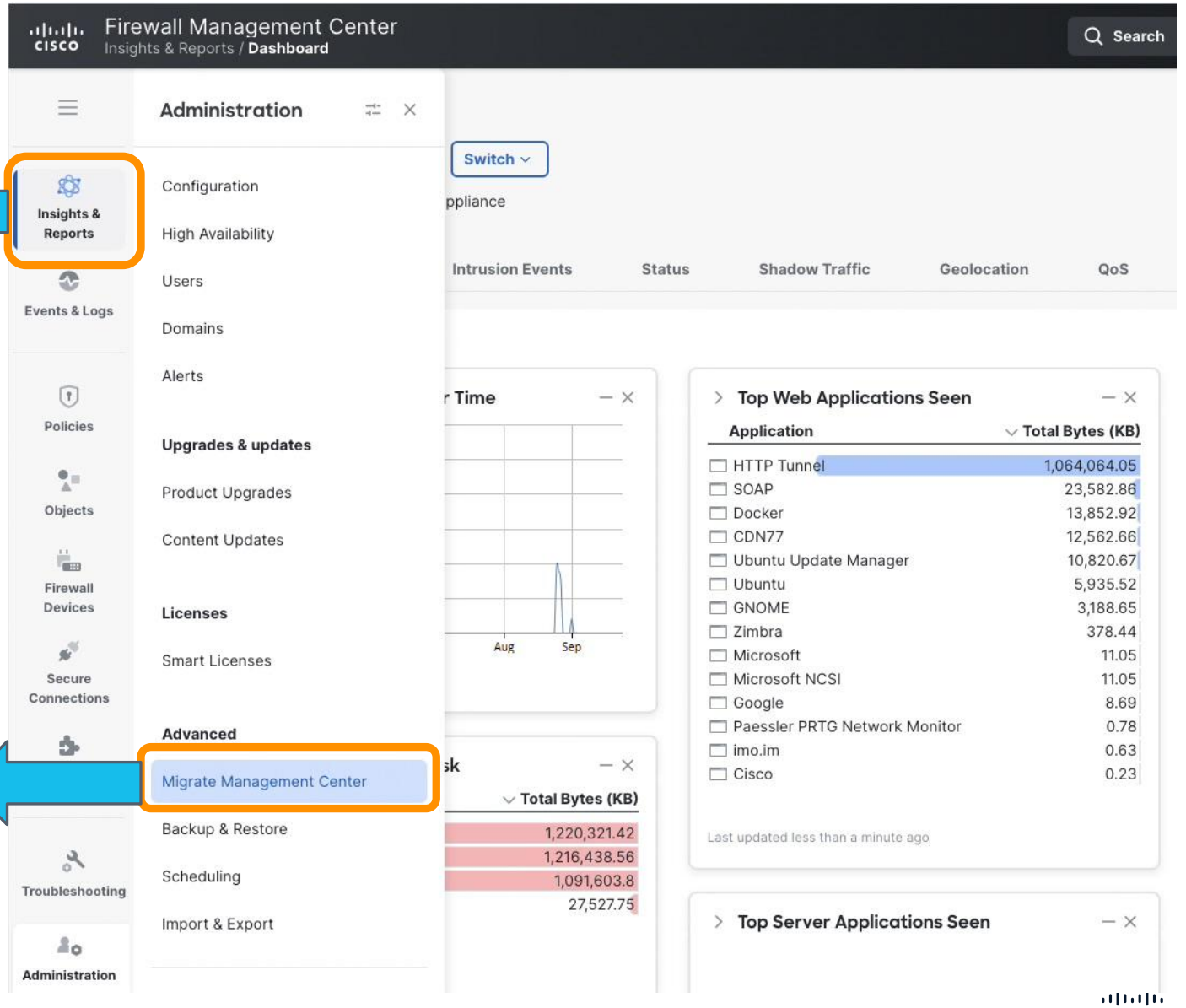
© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)

Option Available under

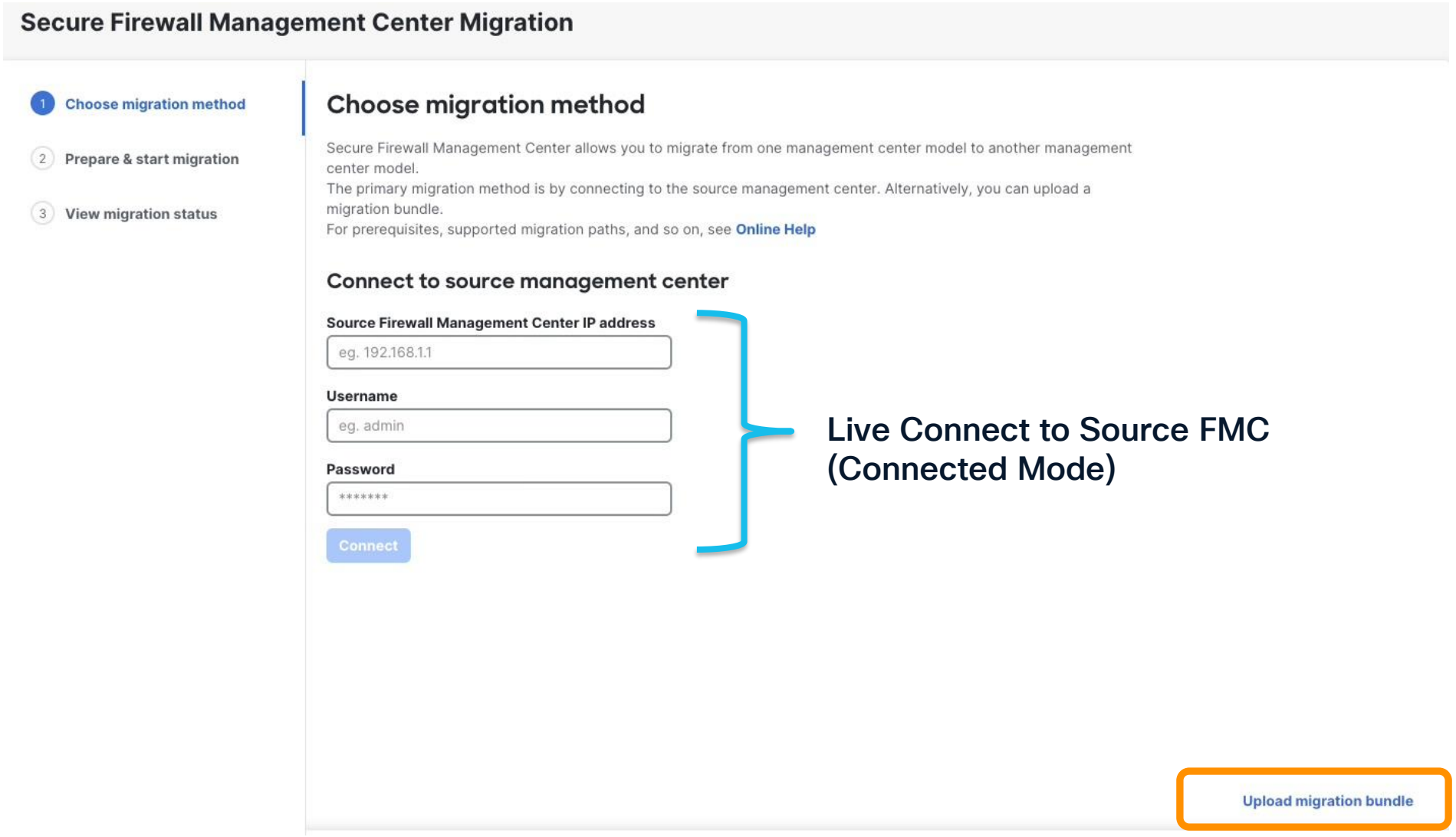
Insights & Reports

Option to migrate the Management Center



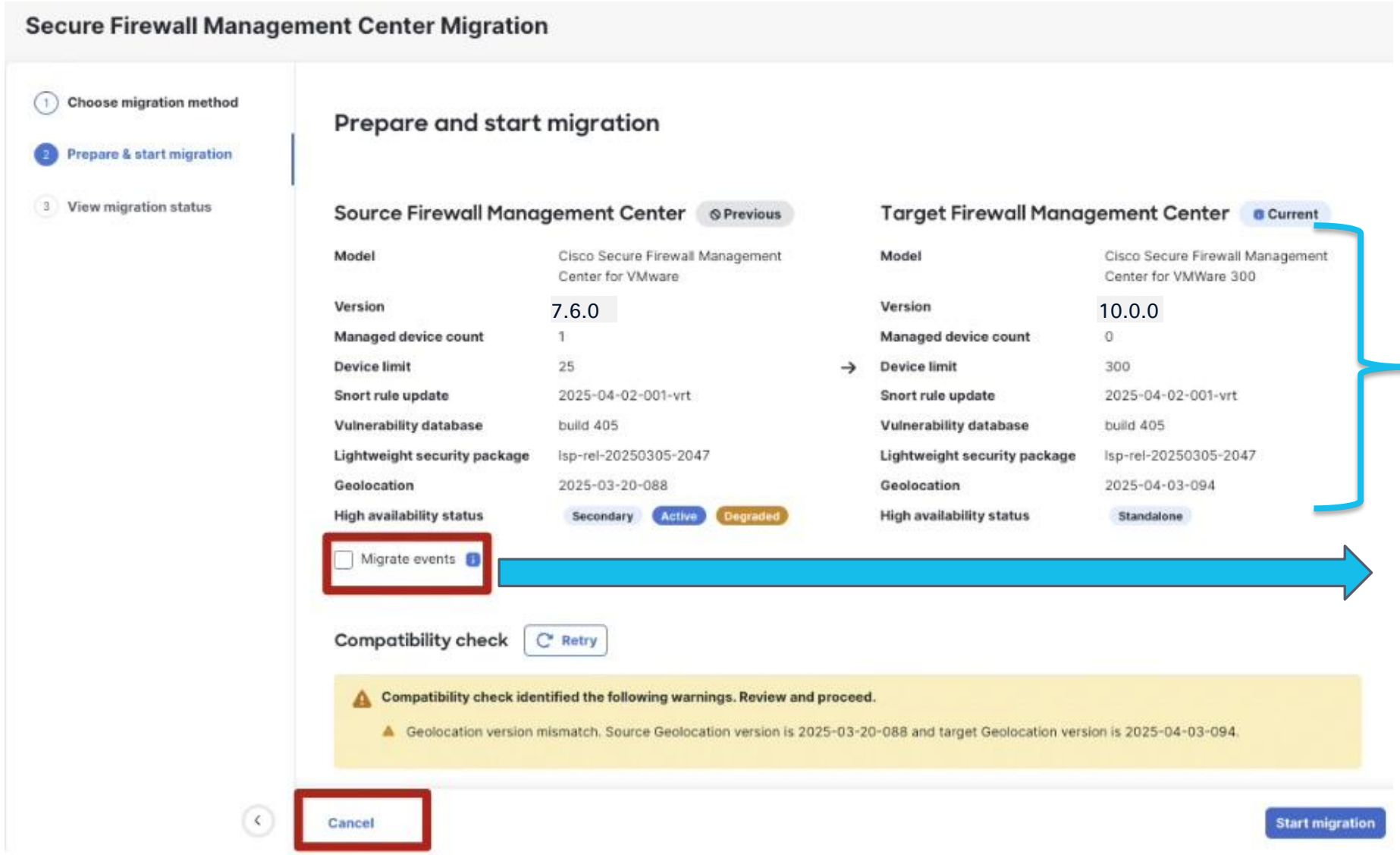
© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)



© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)

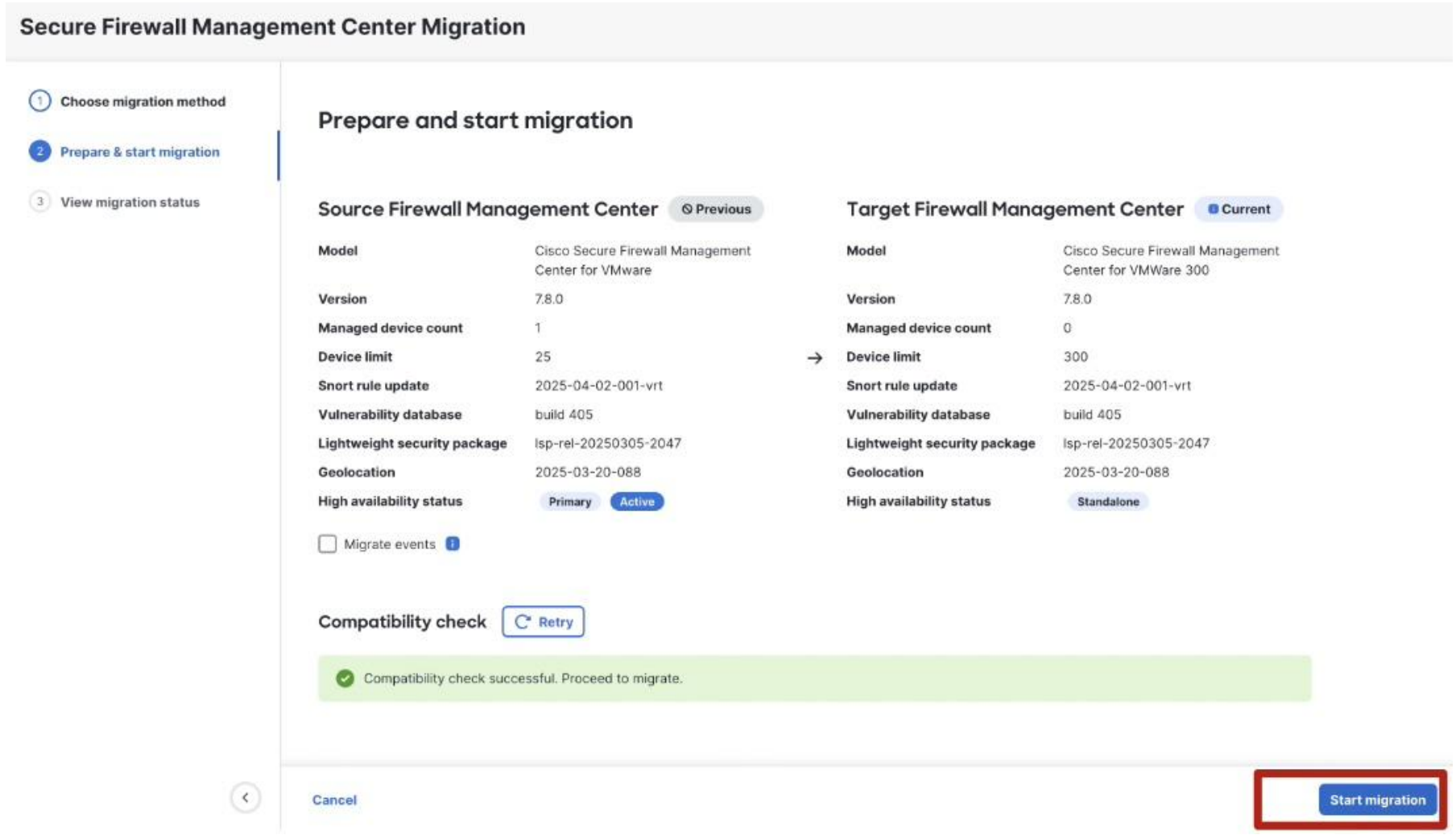


Hardware & Software Details

If events are needed

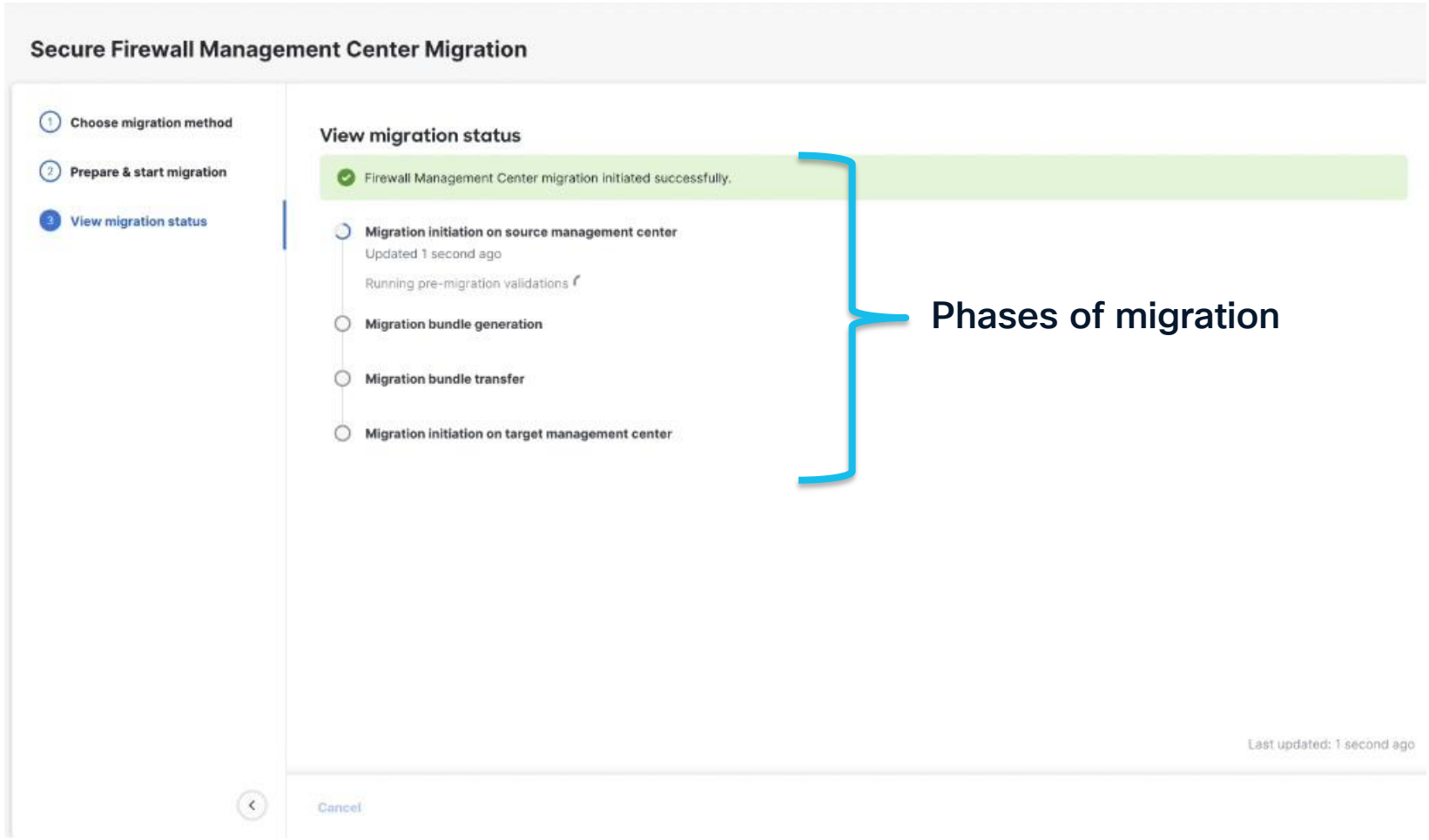
© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)



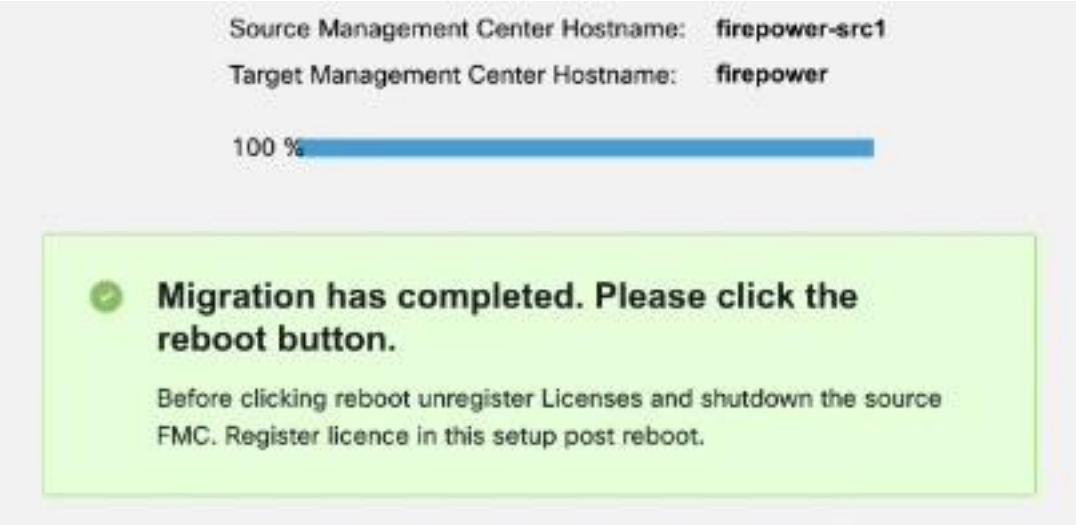
© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)



© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)



© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)

```
root@firepower:/etc/rc.d/modelmigrationboot.d# fmc_model_migration_cli.pl

******** Management Center Model Migration **********

This Management Center information:

Management Center Version : 10.0.0
Model                     : Cisco Secure Firewall Management Center for VMWare 300
UUID                      : 71df26dc-5c8a-11f0-9b2a-2c63491baa60
Managed devices limit     : 300

**************************************************
No TGZ file path provided, using default: /etc/rc.d/modelmigrationboot.d/modelmigrationboot.d.tar.gz
Extracting /etc/rc.d/modelmigrationboot.d/modelmigrationboot.d.tar.gz to /var/tmp/fmc-migration...
Do you want to migrate events? (yes/no): yes
Configuration and events will be migrated.
Do you want to proceed with the migration? (yes/no): yes
Starting migration script...
Migration process started with PID: 32470
You can monitor the progress with /var/log/fmc_migration.log
root@firepower:/etc/rc.d/modelmigrationboot.d#
```

Execute the command at the CLISH

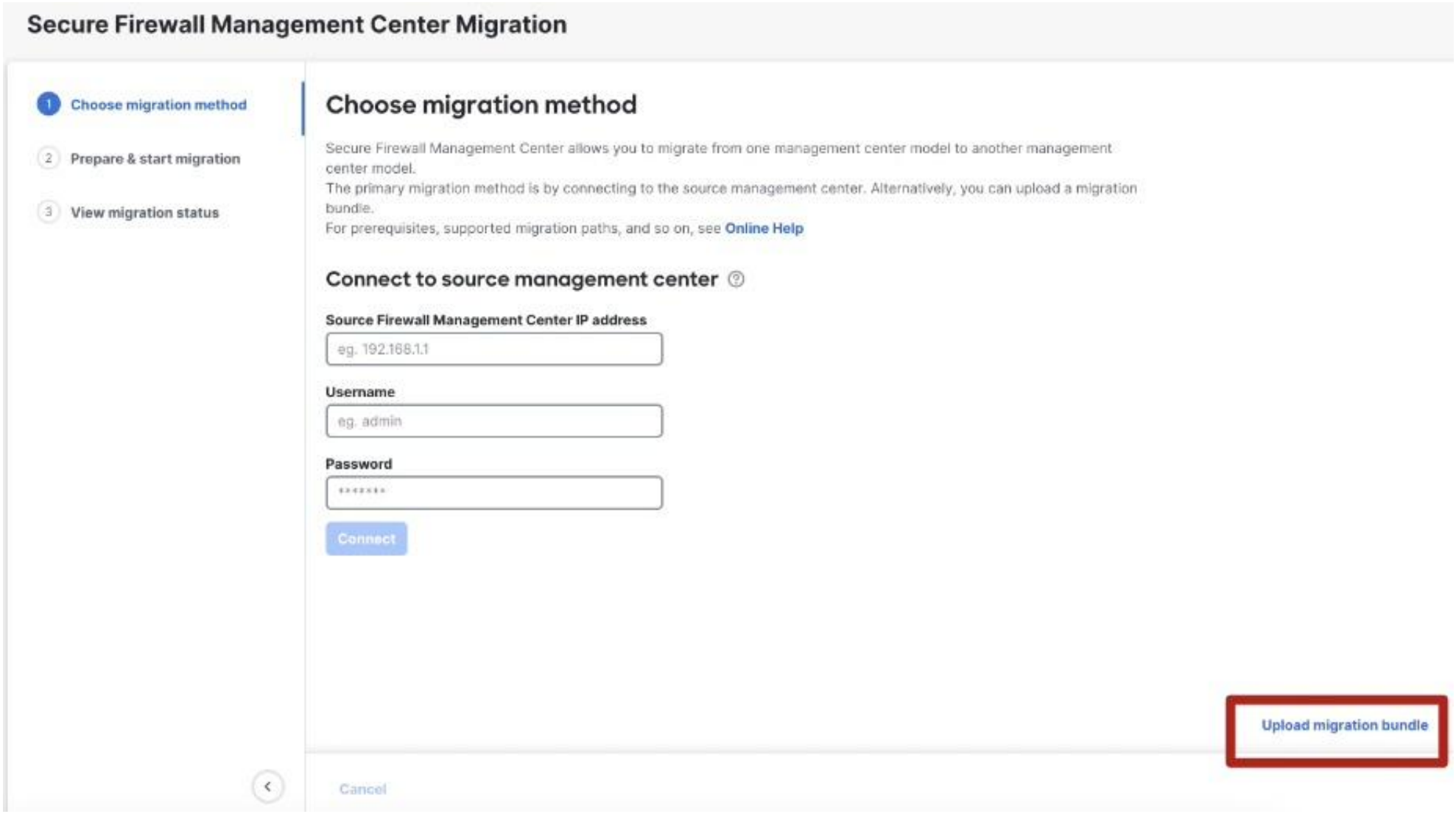
`sudo fmc_model_migration_cli.pl`

Notice that Do you want to proceed with migration answer is “yes”. This starts the operation.

© 2025 Cisco and/or its affiliates. All rights reserved.

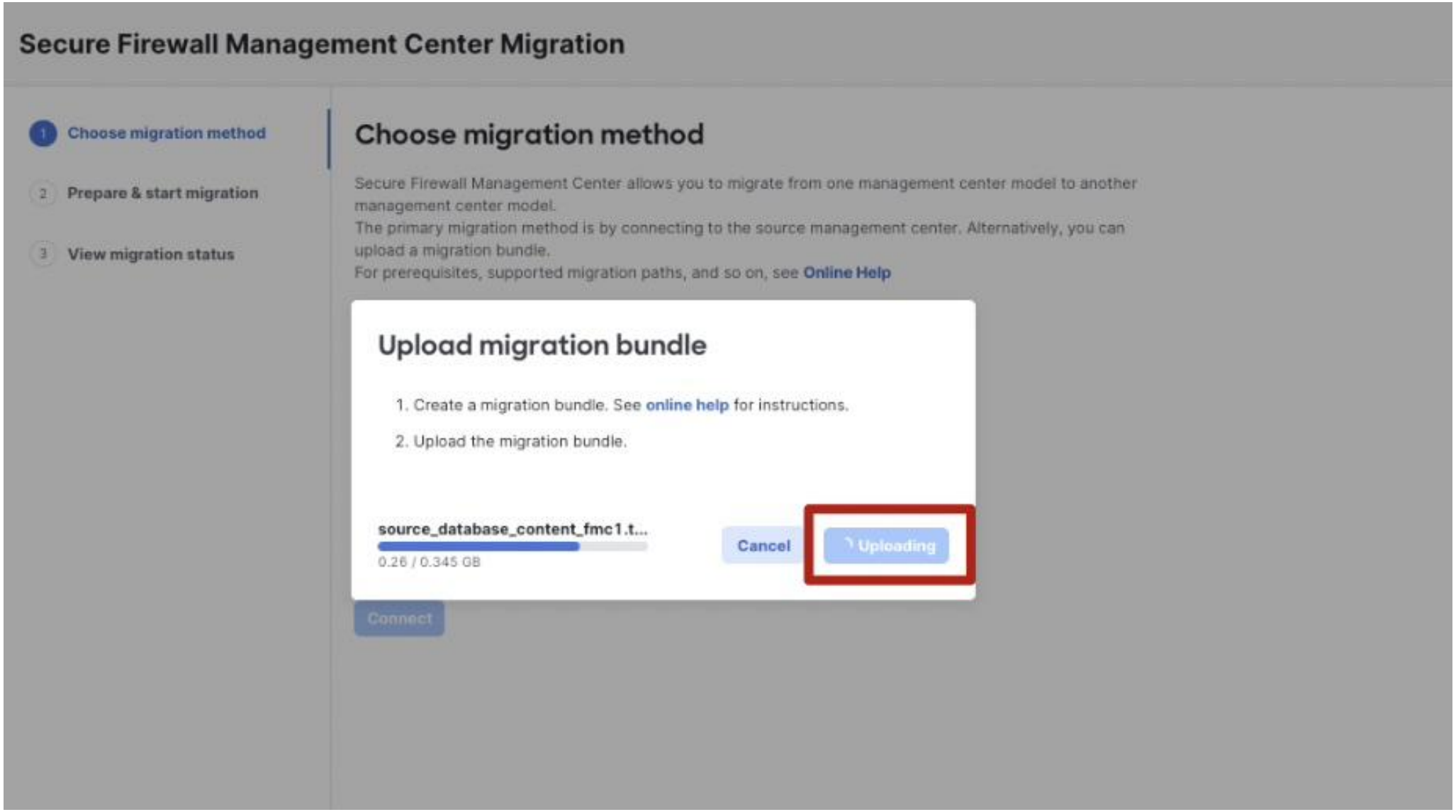
cisco

New Migration Workflow (10.0.0)



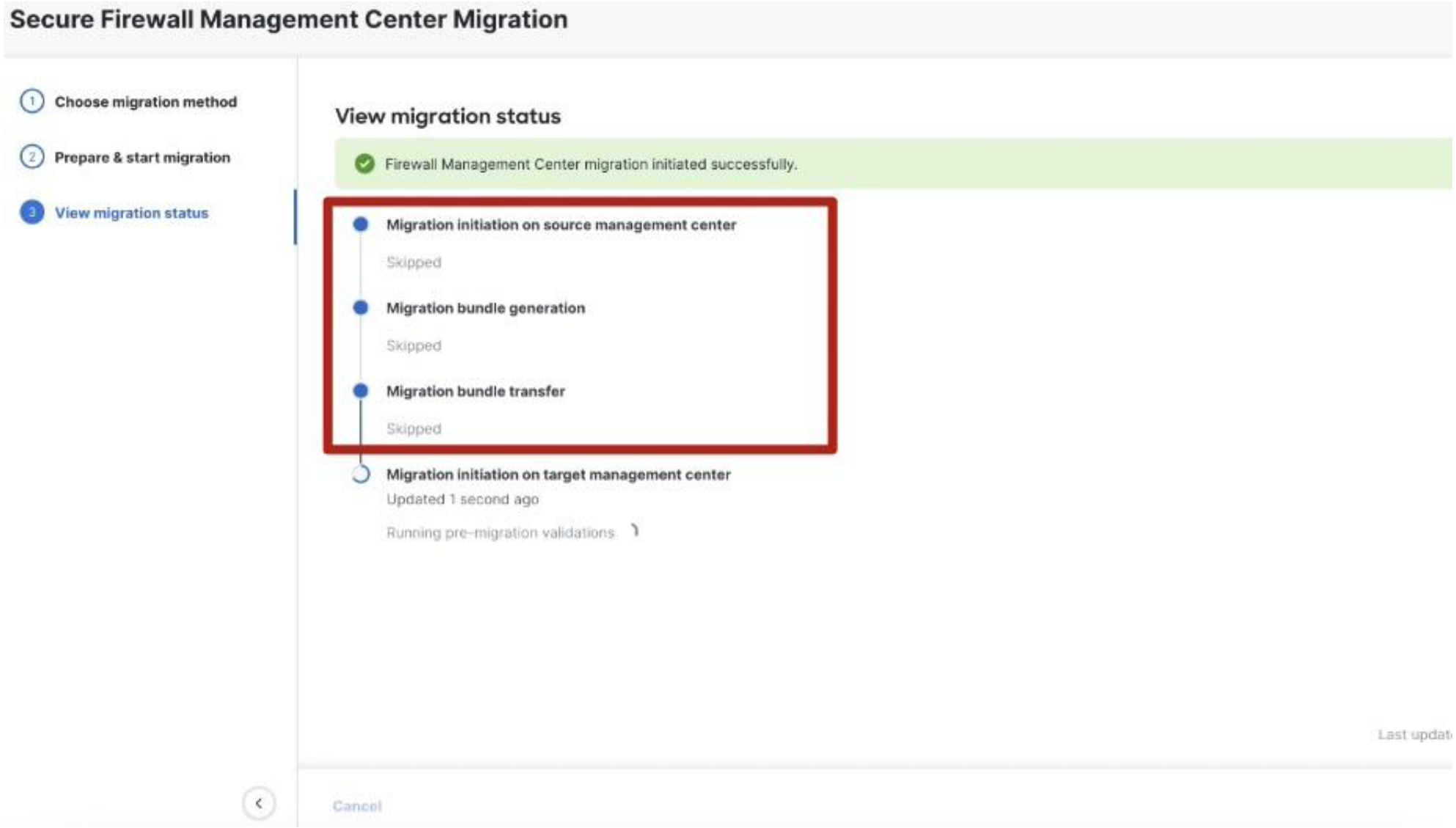
© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)



© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)



© 2025 Cisco and/or its affiliates. All rights reserved.

New Migration Workflow (10.0.0)

FMC HA Model Migration Workflow Overview

- A pair of source FMCs in HA and two standalone target FMCs.

- Overview of Steps
  1. Migrate the Active source FMC Primary to one of the standalone target FMCs.
  2. Deregister Active source FMC Primary from Smart Licensing and shut it down.
  3. Migrate the Standby source FMC secondary to the other standalone target FMC.
  4. Deregister Standby source FMC Secondary from Smart Licensing and shut it down.
  5. Resolve split-brain between the two targets.

© 2025 Cisco and/or its affiliates. All rights reserved.

Migrating FTD to cdFMC

Prepare for Migration

- Upgrade the on-premises FMC/FTD to a SCC-supported version
- Onboard the FMC to SCC
- We support a temporary upgrade from 7.0 to 7.4 (FMC:1000/2500/4500)
- Ensure you have registered the cdFMC with a smart license
- Check for supported features

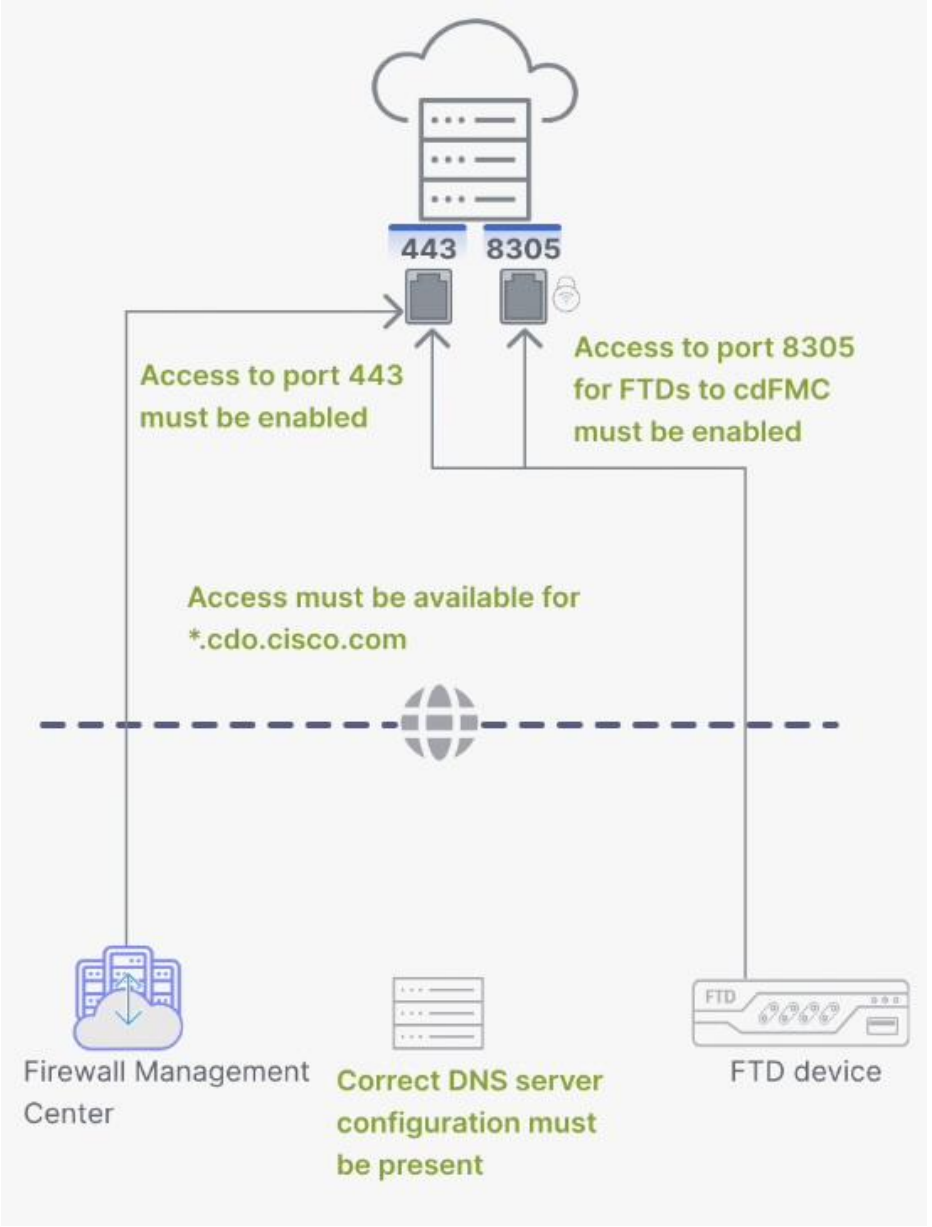
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Points to remember

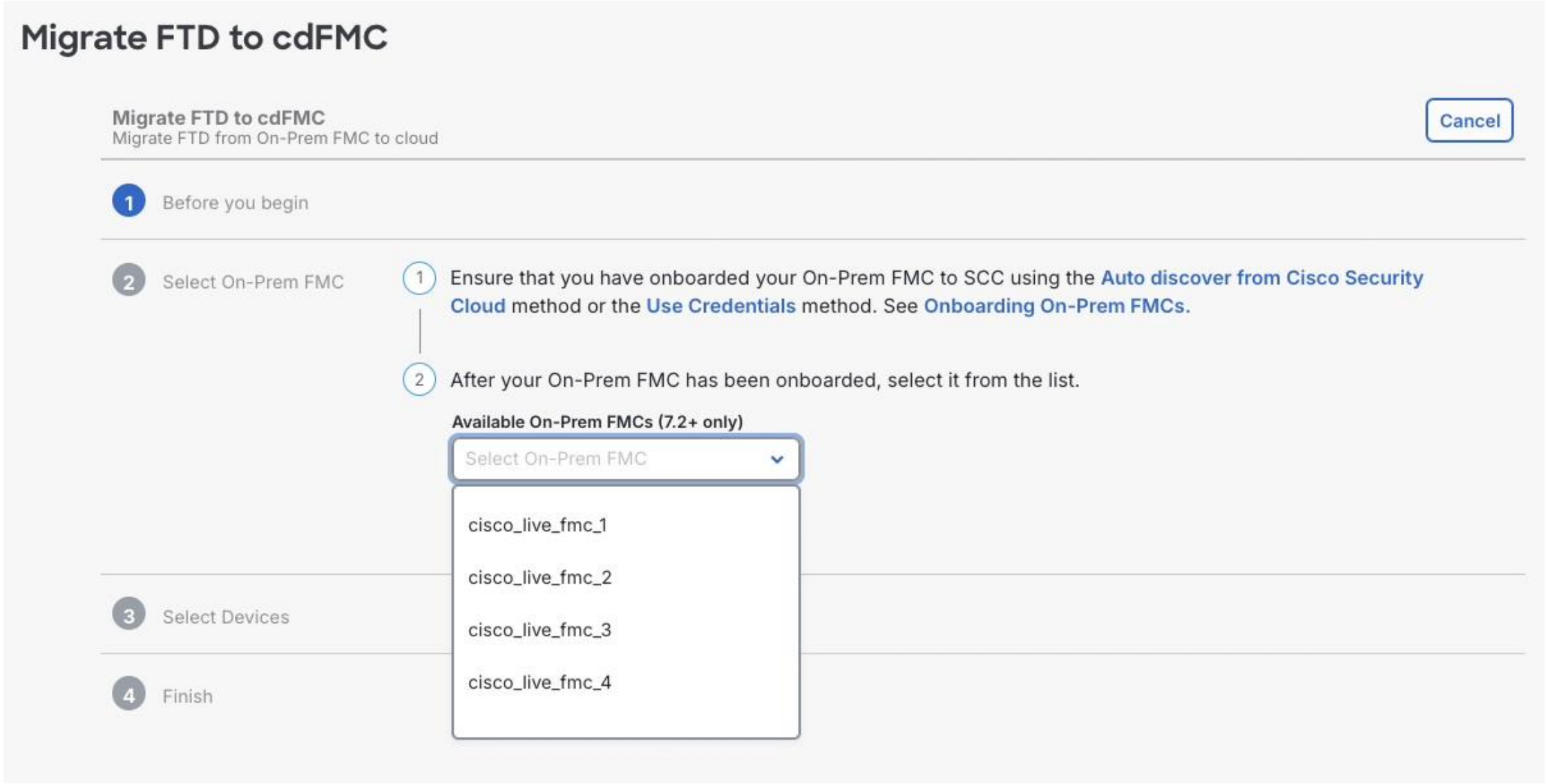
- If a policy in cdFMC shares the same name as one in On-Prem FMC (excluding network, port, URL, and VLAN objects), the cdFMC version will be retained
- After migration, policies and objects aren't auto-synced. For phased migrations, you must update them manually.
- You can revert to On-Prem FMC within 14 days of migration. After that, changes are finalized automatically.

Additional Info



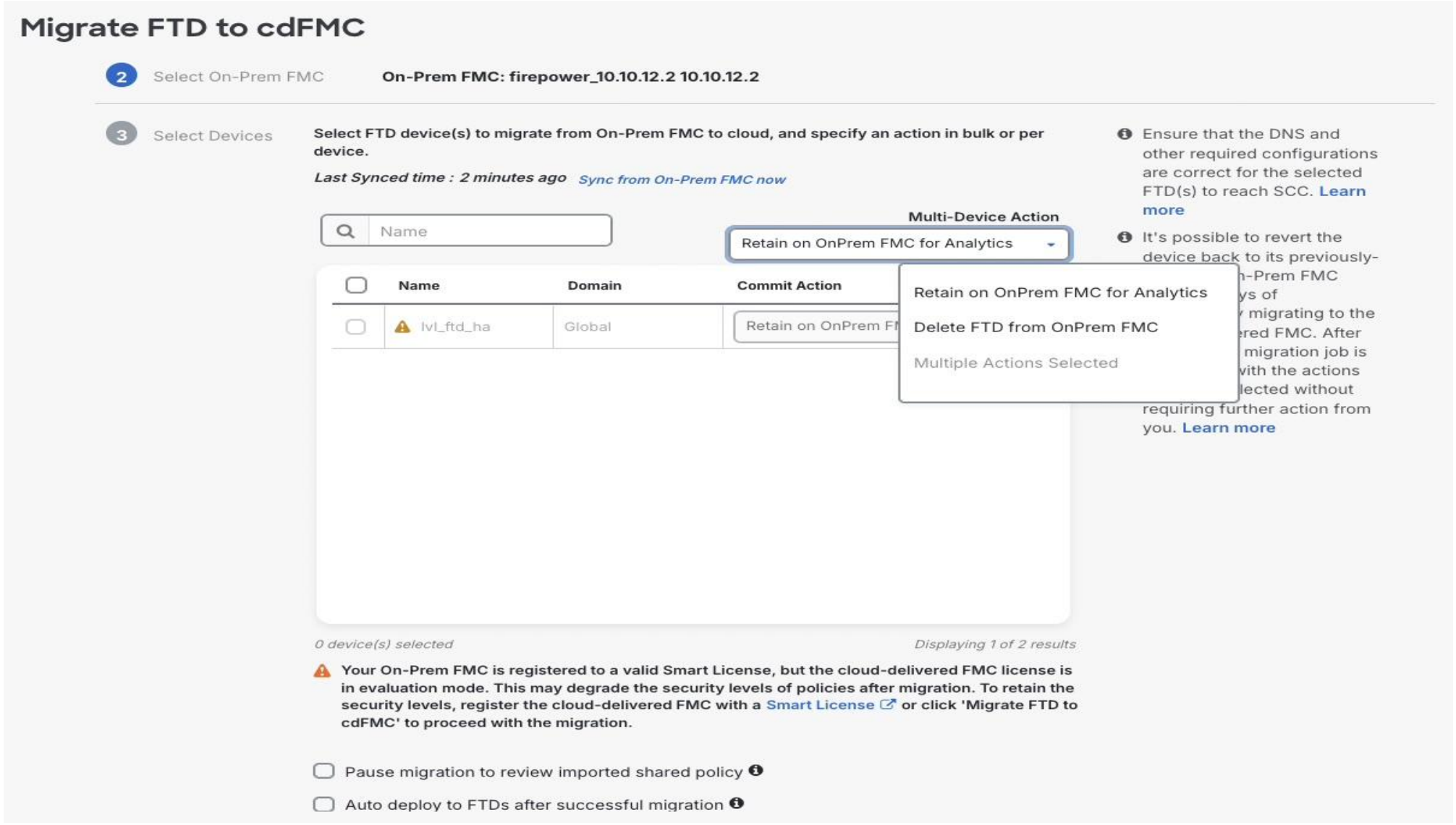
© 2025 Cisco and/or its affiliates. All rights reserved.

Migration Process (1/3)



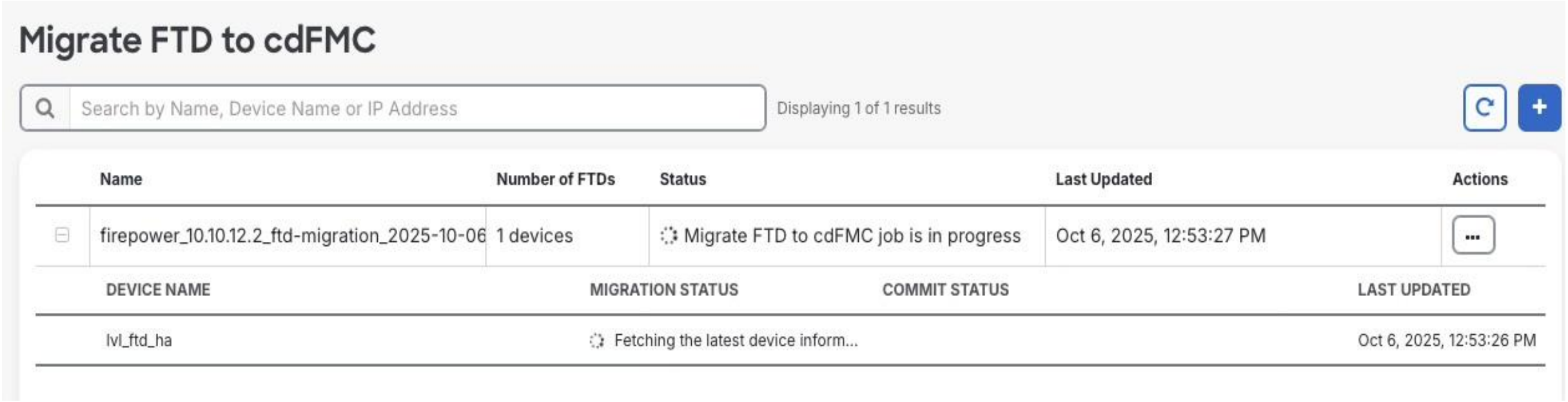
© 2025 Cisco and/or its affiliates. All rights reserved.

Migration Process (2/3)



© 2025 Cisco and/or its affiliates. All rights reserved.

Migration Process (3/3)



© 2025 Cisco and/or its affiliates. All rights reserved.

TAC Insights

Error Reported	Cause	Remediation
Configuration export from On-Premises Firewall Management Center failed	1. Disk space is full or nearly full. 2. Concurrent operations such as device upgrade, upgrade revert, device import and export, or policy analysis are running in on-premises FMC. 3. Connectivity issues exist between the on-premises FMC and SCC.	1. Ensure that at least 10% of disk space is available to accommodate the creation of necessary export files. 2. Ensure that no parallel operations are running during the migration. 3. Ensure that the network connection between on-premises FMC and SCC is stable and reliable.
Failed to commit migration; the device is ineligible	1. The device has pending changes that have to be deployed. 2. The device to be migrated is part of FTD high availability (HA), but the current state is invalid, for example, it is in Active/Active state. 3. The device to be migrated is connected in Analytics-only mode. 4. Cluster migration is supported only for FTDs version 7.4 and above. 5. Migration for chassis and MI FTDs on models 3100/4200 is currently not supported.	1. Verify that the device is up to date with On-Premises FMC. 2. Ensure all pending changes on the devices are deployed. 3. Confirm that the Firewall Threat Defense device is in a valid state

More Insights

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

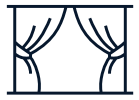
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: raghukul@cisco.com

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

cisco Live !